Universidade de Cabo Verde

IVANDRA MARIA TEIXEIRA CORREIA Nº 2845

Instituição do Estagio:

Universidade de Cabo Verde Campus de Palmarejo

Título do Relatório Projecto Estágio:

SEGURANÇA WIRELESS

O CASO DA UNI-CV

Licenciatura em Tecnologia de Informação e Comunicação

Relatório do final do Curso apresentado na Uni-CV - Campus do Palmarejo para a obtenção do grau de licenciatura em Tecnologias de Informação e Comunicação, sob a orientação de **Mestre ISAÍAS BARRETO DA ROSA (IBR@GMAIL.COM)** e supervisionando por Celestino Barros(celestinoti@hotmail.com) intitulado "Segurança em Rede Wireless".

Uni-CV, 2009

:

O Júri

_____
(O Presidente do Júri)

_____
(O Arguente)

_____
(O Orientador)

Uni-CV, 2009

Dedicatória

Resumo

O relatório apresentado é a base do estágio curricular do curso de Tecnologia de Informação e Comunicação na Universidade de Cabo Verde. Este projecto tem por objectivo apresentar e descrever as actividades de estágio desenvolvidas no Serviço Técnico da Uni-CV, no Campus do Palmarejo, no período compreendido entre 13 de Maio a 28 de Agosto de 2009.

O projecto teve como resultado a integração de rede sem fios no servidor Radius, onde o acesso à rede sem fios é feito mediante a autenticação integrado na active directory;

Para desenvolvimento deste projecto passamos pelas seguintes fases:

- Instalação de Windows server 2003;
- Instalação do active directory;
- Criação do Utilizador;
- Adicionar o utilizador ao grupo;
- Integração de servidor RADIUS no Windows server 2003;
- Instalação da CA,
- Instalação de IAS ,
- Configuração do RADIUS;
- Configuração do acess Point;
- Configuração do Cliente Windows XP;

Índice

Figuras

Glossário

WMAN	Wireless Metropolitan Area Networks
IEEE	Instituto de Electricistas e Electrónicos
DSL	Linha de Assinante Digital
WPAN	Wireless Personal Area Networks
WLAN	Wireless Local Area Network
RADIUS	Remote Authentication Dial-In User Server
EAP	Extensible Authentication Protocol
IAS	Internet Authentication Server
CA	Certificate Services
ACLs	Access Control List
ADUC	Active Directory Users and Computers
AP	Access Point
Wi-Max	Worldwide Interoperability for Microwave Access
WWiSE	World Wide Spectrum Efficiency
SIG	Bluetooth Special Interest Group

Introdução

No âmbito da realização do projecto científico no final do quarto ano do curso para a obtenção do grau de licenciatura em Tecnologia de Informação e Comunicação, escolhemos o tema **“ Segurança em Rede Wireless “**.

As razões que justificam a escolha do tema ora apresentado têm a ver com o estágio realizado para o grau de licenciatura em Tecnologia de Informação e Comunicação no Serviço Técnico da Universidade de Cabo Verde - Campus de Palmarejo, cujo projecto foi “Segurança Wireless na rede da Universidade.

A “s**egurança wireless”** é uma das formas de manter a segurança em redes wireless, porquanto permite controlar o acesso dos utilizadores à rede e aos recursos disponibilizados, garantindo, deste modo, a partilha de recursos de forma racionalizada e que possibilite a cada utilizador ter acesso a recursos necessários para desempenhar a sua função na organização.

1.1 Os objectivos

O **Objectivo Geral** deste trabalho é o contribuir para a melhoria de segurança da rede sem fios no Campus do Palmarejo da Uni-CV, através do desenvolvimento de um mecanismo de encriptação da sua rede wireless.

Os Objectivos Específicos são:

- Compreender o mecanismo de funcionamento de segurança wireless;
- Entender a estrutura de redes da Universidade - Campus do Pamarejo;
- Instalação de um Servidor Radius;
- Integração desse servidor no Active Directory;
- Integração de rede sem fios no servidor radius e Windows server 2003 ficando o acesso a rede sem fios feito Mediante a Autenticação integrado na active directory ;

1.2 Técnicas Utilizadas

As técnicas Utilizada para realização deste trabalho são:

- Pesquisa Bibliográfica;
- Estudo de Caso.

1.3 Estrutura de trabalho

O trabalho inicia-se com a **Introdução** onde se faz a referência ao tema do trabalho, os objectivos gerais e específicos a tecnicas utilizada e por fim a estrutura de trabalho.

No primeiro capitulo – **Rede Wireless** apresenta aos seus conceitos básicos, aparecimento de rede wireless, conceito e tipos de rede wireless, vantagem e desvantagens de rede wireless, equipamentos de rede wireless e por último padrões para rede wireless.

No segundo capitulo – **Segurança wireless** expõe-se seus aspectos históricos, conceito de segurança wireless, as principais ameaças de rede wireless, técnicas de protecção de redes wireless, riscos e vulnerabilidades de rede wireless, segurança Física e por ultimo a localização do acess point.

No terceiro Capitulo – **O Caso da Universidade de Cabo Verde – Campus de Palmarejo** começa-se primeiramente por um enquadramento depois a descrição da Uni-CV, Organograma da Empresa, Infra-Estrutura ds TIC da Uni-CV, desenho lógico do sistema, requisitos necessários, ferramentas utilizadas para o trabalho, Etapas de realização do trabalho e por último considerações Finais

Por ultimo o capitulo de **conclusão** faz se abordagem geral do trabalho.

capítulo 1: Rede Wireless

1.1 Aparecimento da Rede Wireless

Para Lopes et al, (2008), as redes sem fio nasceram da mesma maneira que muitas outras tecnologias nasceram no meio militar. Tinha uma precisão de implementação de uma rede simples e segura para troca de informações em ambiente de luta. O tempo foi-se e a tecnologia evoluiu, deixando de ser limitada para o meio militar passou a ser alcançável ás empresas, universidades, autoridades e aos utilizadores privados. Hoje podem se considerar "redes sem fio" como uma opção muito atraente em relação às redes cabeadas, pois apesar de custo elevado, as suas aplicações são numerosas e diversas.

Para ter uma comunicação preferível entre redes distintas, as redes sem fio foram padronizadas para permitir a comunicação entre os equipamentos de marca diferentes, ter uma melhor segurança, redução de custo e também ter a possibilidade de fazer actualizações ou melhorias nos equipamentos

1.2 Conceito de Rede Wireless

Palavra Wireless, provém do inglês: wire (fio, cabo); less (sem); ou seja: sem fios.

Wireless é qualquer tipo de conexão para transmitir informação sem a utilização de fios ou cabos. (Tomé, 2003)

Segundo este Autor o controlo remoto de televisão ou aparelho de som, telefone celular e muitos outros aparelhos trabalham com conexões wireless. Podemos dizer, como exemplo prático, que durante uma conversa entre duas pessoas, temos uma conexão wireless, partindo do princípio de que sua voz não utiliza cabos para chegar até o receptor da mensagem.

1.3 Tipos de Rede Wireless.

De acordo com Brasil (2004), existem vários tipos de redes sem fio que variam em tecnologia e aplicação, é possível classificá-las em quatro tipos:

- WLAN (Wireless Local Area Network)
- WMAN (Wireless Metropolitan Área Network)
- *WPAN* (Wireless Personal Area Networks)
- *WWAN* (Wireless Wide Area Network)

As redes locais sem fio (Wireless Local Area Netowrk) são padronizadas pelo IEEE 802.11 Wireless Local Area Network Working Group. São redes com uma pequena dispersão geográfica e altas taxas de transmissão. As WLANs têm uma grande agilidade para seus utilizadores, principalmente para os que usam computadores portáteis.

As redes metropolitanas sem fio (Wireless Metropolitan Area Networks) são definidas pelo padrão IEEE 802.16 e também é conhecida como rede sem fios de banda larga. A WMAN é a principal concorrente da fibra óptica, pois possui como diferencial, devido á sua grande mobilidade, alcance e disponibilidade que são serviços considerados superiores aos serviços de DSL (*Digital Subscriber Line* – Linha Digital para Assinantes) existentes, pois este possui uma limitação em sua distribuição relacionada a distâncias e custos.

As redes pessoais sem fio (Wireless Personal Area Networks) são definidas pelo padrão Bluetooth, que actualmente é associado no padrão IEEE 802.15. são voltadas, principalmente, para a conexão de um computador a dispositivos periféricos, como impressoras, PDAs (Personal Digital Assistants) e telefones celulares, eliminando a necessidade de cabos. As WPANs alcançam pouca distância e oferecem baixas velocidades, se comparada a outras tecnologias wireless.

As redes distribuídas sem fio (Wireless Wide Area Network) são redes com grande espaço geográfico, voltadas para aplicações móveis que utilizem telefones celulares. Existem inúmeras tecnologias para WWANs que limitam a taxa de transmissão e, consequentemente, o tipo de serviço que poderá ser oferecido. As redes de celulares estão caminhando rapidamente para tornarem-se a maior aplicação de WWAN. Com o crescente uso de conexões de banda larga, celulares estão transmitindo emails, textos, imagens, som e vídeo, com a mesma qualidade e velocidade que os dispositivos ligados por fios.

1.4 Vantagens e desvantagens de Rede Wireless

Para Silva (S/D), as redes sem fios apresentam inúmeras vantagens tanto para os utilizadores como para a empresa de uma forma geral. Tais como:

- Maior mobilidade
- Maior escalabilidade
- Instalação rápida e simples
- Alta imunidade a ruídos
- Conexão permanente
- Não usa a linha telefónica
- Baixo custo de manutenção

Ao falar das vantagens da rede sem fios pode-se dizer que é uma rede com muita mobilidade dando aos seus utilizadores acesso à informação em tempo real em qualquer espaço é ainda é uma rede escalável porque pode ser configurado com diferentes topologias. Estas configurações podem ser facilmente modificadas e as distancias entre as estações adaptadas desde poucos utilizadores até centenas (Júnior, 2003)

A instalação de uma antena externa e de um rádio no servidor é rápida e simples levando até 15 dias para a sua instalação.

As redes sem fio têm alta imunidade a ruídos porque utilizam rádios que trabalham na frequência 2,4 GHz. Eles trabalham num sistema de alta frequência ou (frequence hope), o que diminui rapidamente a possibilidade de interferências, garantindo a qualidade do sinal e a integridade das informações. Como é utilizada uma frequência muito alta, o sistema é livre a chuvas, raios e outras interferências de fenómenos meteorológicos.

Pode-se estar permanentemente conectado a Internet com WIP, ou seja, se pode estar On-line vinte e quatro horas por dia, sete dias por semana.

Ainda, com esta rede a linha telefónica fica livre enquanto se navega na Internet. Não se paga a tarifação de pulso telefónico e o custo fixo mensal de um link Wireless é menor do que aquele fornecido por Telecom, com a mesma velocidade.

Por outro lado segundo Júnior (2003), as redes sem fio possuem algumas desvantagens na sua utilização tais como:

- Adaptadores Ethernet com alta rapidez que são, em geral, 10 vezes mais baratos que adaptadores para redes sem fio. A instalação de redes sem fio reduz significativamente os custos mensais de telecomunicações o que proporciona uma rápida recuperação do capital investido nestes equipamentos.

- Qualidade de serviço: a qualidade do serviço oferecido ainda é menor que a das redes cabeadas. Tendo como principais razões para isso a pequena banda passante devido às limitações da radiotransmissor e a alta taxa de erro devido à interferência.

- Pouca largura de banda: Largura de banda comparada com a rede física tradicional apresenta até hoje, pouca largura de banda.

- Segurança e privacidade, quando esta rede não for bem implementada pode ser vulnerável permitindo a captura de informações ou de dados por parte de terceiros já que utiliza interface de rádio aberta e é muito mais fácil de ser ludibriada do que sistemas físicos tradicionais. Para solucionar esta vulnerabilidade deve-se sempre utilizar a criptografia dos dados através de protocolos tais como WEP ou IPsec.

- Restrições: Cada país tem a sua regulamentação e restringem a operação das faixas de frequência para que a interferência seja minimizada, por isso, todos os produtos sem fio precisam respeitar os regulamentos locais. Um grande obstáculo para o uso dos equipamentos Wireless é a necessidade de confirmação directa entre os pontos.

1.5 Equipamentos Wireless.

Para Lopes et al (2008), existem vários tipos de equipamento wireless.

- Access Point
- Bridge
- Antenas
- Pontes Wireless Workgroup
- PC Card
- Placas PCI

- **O Access Point** é um equipamento armado com um rádio transmissor/receptor que actua como um bridge transparente, permitindo a comunicação entre dispositivo wireless e uma estrutura de rede concertada, com taxas de até 11 Mbps.Ainda pode ser utilizado para interligar duas redes remotas, através de um link de rádio, diminuindo bastante os custos de comunicação e viabilizando a integração dos sistemas administrativos devido à grande largura de banda suportada. Concentra todo o tráfego da rede wireless além das conexões oriundas dos clientes. Possui um identificador que identifica a rede chamado SSID.

- **Bridge** é um equipamento que interliga duas redes locais (LANs) ou dois segmentos de uma mesma LAN. Os bridges são protocolo-independente, enviando pacotes sem a capacidade de optimizar rotas. Isso lhes dá velocidade, mas muito menos versatilidade.Conectam duas ou mais redes, compreende 4 modos de operação: Root, Non-Root, Access Point e Repeater. Tem uma capacidade de formação de backbone wireless através de 2 PC Cards.

- **As Antenas** podem ser conectadas a acess point ou a máquinas clientes para aumentar o ganho do sinal e assim melhorar a transmissão de dados. Podem ser direccionais ou omnidireccionais. Uma antena é direccional quanto menor for a largura do feixe e mais longe for o sinal resultando em um alcance maior. As antenas direccionais concentram o sinal em uma única direcção. Seus sinais podem ter alcance curto e amplo, ou longo e estreito. Via de regra, quanto mais estreito o sinal, maiores distâncias ele alcançará. Normalmente, este tipo de antena é utilizado em estações remotas para fazer a comunicação entre estas estações com uma ou mais estações base. Uma antena é omnidireccionais quando tem um alcance menor e possuir uma largura de feixe maior. As antenas omnidireccionais cobrem 360º no plano horizontal. Trabalham excepcionalmente bem em áreas amplas ou em aplicações multiponto. Normalmente, este tipo de antena é utilizado em estações base, com estações remotas colocadas ao seu redor.

- **Pontes Wireless Workgroup** agrupam vários clientes LAN e transforma essa LAN em único cliente WLAN.É recomendado em situações em que um pequeno grupo de utilizadores necessita de acesso a rede principal. O número máximo de estações que pode ser conectado está compreendido entre 8 e 128, dependendo do fabricante.

- **PC Card** é usado somente em notebooks, serve para conectar o notebook a rede wireless e possui uma antena interna embutida;

- **As Placas PCI** é usado somente em desktops, serve para conectar o desktop a rede wireless. A sua antena é externa e acoplada a saída de placa;

1.6 Padrões para rede sem fios

Existem vários padrões internacionais para a rede sem fios e, entre elas, podem destacar-se:

1.6.1 Padrão 802.11b

O 802.11b utiliza distribuição fantástica por sequência directa para receber e transmitir os dados a uma velocidade máxima de 11 megabits por segundo, porém esta não é sua velocidade real, pois estes 11 Mbps incluem toda sobrecarga de rede para o início e o fim dos pacotes. A taxa real pode variar de acordo com as configurações do equipamento em que se encontra, porém pode variar entre 4 a 7 Mbps aproximadamente. (Lopes et al, 2008)

1.6.2 Padrão 802.11a

Chega a alcançar velocidades de 54 Mbps dentro dos padrões da IEEE e de 72 a 108 Mbps por fabricantes não padronizados. Esta rede opera na frequência de 5 GHz e inicialmente suporta 64 utilizadores por Ponto de Acesso (PA). As suas principais vantagens são a velocidade, a gratuidade da frequência que é usada e a ausência de interferências. A maior desvantagem é a incompatibilidade com os padrões no que diz respeito a Access Points 802.11 b e g, quanto a clientes, o padrão 802.11a é compatível tanto com 802.11b e 802.11g na maioria dos casos, já se tornando padrão na fabricação dos equipamentos. (Ono, 2004)

1.6.3 Padrão 802.11g

É o mais recente padrão para redes sem fio. Actua na banda ISM de 2.4 GHz e provê taxas de transferências de até 54 Mbps. Tem os mesmos inconvenientes do padrão 802.11b (incompatibilidades com dispositivos de diferentes fabricantes). As vantagens também são as velocidades). Usa autenticação WEP estática já aceitando outros tipos de autenticação como WPA (Wireless Protect Access) com criptografia dinâmica (método de criptografia TKIP e AES). Torna-se por vezes difícil de configurar, como Home Gateway devido à sua frequência de rádio e outros sinais que podem interferir na transmissão da rede sem fios. (Gemines, 2005).

1.6.4 Padrão 802.11.16 (Wi-Max)

Sua principal utilização e finalidade de criação é alcançar longas distâncias utilizando ondas de rádio, pois a utilização de cabos de rede para implementação de uma rede de dados de alta velocidade a uma distância longa, seja ela entre cidades, em uma residência ou em uma área rural, por exemplo, pode custar muito caro e estar ao alcance financeiro de poucos.
Visando desenvolver um padrão para atender esta demanda, o IEEE no seu papel de precursor da padronização, cria o padrão 802.16 (Albuquerque, 2008)

1.6.5 Padrão 802.11n

Este padrão ainda está em fase de definição tendo como principal finalidade o aumento da taxa de transmissão dos dados, algo próximo dos 100 a 500 Mbps. Este padrão também é conhecido como WWiSE (World Wide Spectrum Efficiency). Tem como objectivo alcançar um elevado aumento na área de cobertura do sinal. O padrão 802.1n pode operar com canais de 40 Mhz, e manter compatibilidade com os outros que trabalham em 20 Mhz, porém suas velocidades varia em volta de 135Mbps[1]

[1] http://www.oficinadanet.com.br/artigo/988/redes_sem_fio_padrao_ieee_802.11 acessado em 13/08/2009

1.6.6 Padrão 802.1x

O 802.1X é uma estrutura baseada nos padrões IEEE para autenticar o acesso a uma rede e, opcionalmente, gestão de chaves usadas para proteger o tráfego. O 802.1X depende de um RADIUS (Remote Authentication Dial–In User Service), uma autenticação de rede e um serviço de autorização para verificar as credenciais do cliente na rede. O 802.1X utiliza o EAP como meio de fazer o pacote de conversação da autenticação entre diversos componentes da solução e gerar as chaves usadas para proteger o tráfego entre os clientes e o hardware de acesso da rede. (kaminski, salimen e Dhamer, 2007)

capítulo 2: Segurança Wireless

2.1. Aspecto Históricos

A segurança é um dos temas mais importantes das redes sem fio. Desde seu surgimento, vêem tentando disponibilizar protocolos que garantam as comunicações, mas nem sempre isto funciona.

A questão da segurança deve ser muito bem analisada quando se utiliza um sistema em rede, onde vários utilizadores têm acesso. Logicamente, como se tratam de tecnologias que possuem características próprias e/ou únicas, cada uma delas têm as suas vantagens e desvantagens.

Existem riscos potenciais de segurança com as comunicações sem fio, uma vez que um invasor não precisa de acesso físico à rede com fio tradicional para acessar os dados.
Embora as comunicações sem fio compatíveis com a especificação 802.11 não possam ser recebidas por simples scanners ou receptores de ondas curtas, as informações podem ser capturadas por equipamentos especiais ou outros dispositivos 802.11. A segurança da rede é obtida através de vários métodos de autenticação. (Leite, 2007)

2.2. As Principais Invasões ou Ameaça de rede wireless

Para Medeiro (2001), as redes sem fios estão sujeitas a várias ameaças e ataques. Entre elas podemos destacar:

- Espionagem dos dados transmitidos: pode resultar na revelação de dados confidenciais, revelação de credenciais de utilizadores desprotegidas e potencial de roubo de identidade. Também permite que habilidosos utilizadores mal intencionados traxem informações sobre seus sistemas de TI, as quais podem ser usadas para organizar um ataque a outros sistemas ou dados que poderiam não estar vulneráveis.

- Interceptação e modificação de dados transmitidos- caso um invasor obtenha acesso à rede, poderá inserir um computador invasor para interceptar, modificar e retransmitir as comunicações entre duas partes legítimas.

- Spoofing (Falsificação) - como sendo uma técnica utilizada por invasores para conseguirem se autenticar a serviços, ou outras máquinas, falsificando o seu endereço de origem. Ou seja, é uma técnica de ataque contra a autenticidade, uma forma de personificação que consiste em um utilizador externo assumir a identidade de um utilizazdor ou computador interno, actuando no seu lugar legítimo. (Medeiros, 2001)

- Parasitismo não há nada mais sinistro do que um intruso usar sua rede como um ponto de acesso livre para a Internet. Apesar de não ser tão danoso quanto algum das outras ameaças, essa poderá, no mínimo, reduzir o nível de serviço disponível para seus utilizadores legítimos.[2]

- Wardriving - Esta forma de invasão foi definida por Peter Shipley para designar a arte de dirigir um automóvel à procura de redes sem fio abertas. Para isto, é necessário um automóvel, um computador com uma interface wireless (um notebook por exemplo) configurada em modo "promíscuo" (o dispositivo detecta, efetua a intercepção e leitura dos dados em qualquer rede wireless de maneira completa). "Tal atividade não

[2] http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod168.mspx

é danosa em si, pois alguns se contentam em encontrar a rede wireless desprotegida, enquanto outros efetuam login e uso destas redes, o que já ultrapassa o escopo da atividade"

- Warchalking- Consistem em símbolos de giz ou carvão em paredes, calçadas, cercas, indicando que naquele local tem um ponto de rede wireless, mostrando suas configurações.

2.3. Técnicas de protecção de rede wireless.

2.3.1 Criptografia

Para Aguiar (2005), a criptografia é utilizada para codificar os dados antes que este sejam transmitidos.
A criptografia vem sendo muito utilizada, principalmente para fins militares e diplomáticos. Em relação computacional, a técnica da criptografia surgiu da necessidade de se enviar informações sensíveis através de meios de comunicação não confiáveis e é utilizada para garantir a segurança em um ambiente computacional que precisa de sigilo das informações.

Os sistemas de criptografia podem ser de dois tipos: Simétrica e assimétrica

2.3.2 Criptografia Simétrica

Criptografia de chave simétrica, é um sistema que utiliza apenas uma chave para codificar e descodificar as informações sensíveis. Assim tanto emissor e receptor conhecem a chave utilizada (Medeiros, 2001)

Segundo Sousa (2002), a segurança desse método é o questionário, pois depende de como a chave é informada entre transmissores e receptor, e como é feita a protecção contra terceiros que podem descobri-la em arquivos ou transmissões da chave.
Um algoritmo simétrico é muito utilizado para criptografia dos dados nas transmissões em redes de computadores é o DES (data encryption satndart) que utiliza um string alfanumérica como chave para codificar e descodificar a mensagem.

2.3.3.Criptografia assimétrica

Segundo este Autor Criptografia assimétrica, ou criptografia de chave-pública, é um sistema que utiliza duas chaves diferentes, uma chave que chama secreta e outra chamada pública. O par de chaves pertence a uma entidade ou pessoa e é calculado a partir de um número aleatório.

Qualquer uma das chaves é utilizada para cifrar uma mensagem e a outra para decifrá-la. As mensagens cifradas com uma das chaves do par só podem ser decifradas com a outra chave correspondente. A chave privada deve ser mantida secreta, enquanto a chave pública disponível livremente para qualquer interessado.[3]

2.3.4 WEP (Wired Equivalent Privacy)

WEP foi o primeiro protocolo usada para criptografia os pacotes de dados de uma rede wireless. WEP é baseado no método de criptografia RC4 da RSA que usa um vector de 24 bits e uma chave secreta distribuída de 40 ou 104 bits. Esta chave é relacionada com a secret shared key para formar uma chave de 64 ou 128 bits que é usada para criptografar os dados. Existem dois padrões WEP, de 64 e de 128 bits (WEP2). O padrão de 64 bits é suportado por qualquer ponto de acesso ou interface que siga o padrão WI-FI (Wireless Fidelity), o que engloba todos os produtos comercializados actualmente. O padrão de 128 bits por sua vez não é suportado por todos os produtos. (Abras, et al 2002)

[3] http://www.training.com.br/lpmaia/pub_seg_cripto.htm aessado em 18/08/2009

2.3.5 WAP2 (Wireless Application Protocol)

Para Nóbrega (S/D), O WAP (Wireless Application Protocol) – é um tipo de Protocolo para Aplicação de rede sem fios, que surgiu para corrigir as vulnerabilidades do WEP, Esse padrão possui uma chave detectora de erros chamada Michael, que é um vector de inicialização de 48 bits, ou seja, o dobro do WEP que tem 24 bits. Possui também um mecanismo de distribuição de chaves.

O WAP possui vantagem que é a melhoria no processo de autenticação de utilizadores da rede, que através de um servidor de autenticação central faz a autenticação de cada um dos utilizadores antes de este ter acesso à rede.

2.3.7 Bloqueamento através de endereço MAC/IP

Para que uma rede funcione de forma eficiente e eficaz, cada dispositivo da rede deve ter uma identificação, para que o equipamento que está a controlar a rede possa ter a capacidade de realizar uma organização da rede. Essa identificação foi definida pelo Institute of Electrical and Electronics Engineers (IEEE), com um número único para cada dispositivo fabricado mundialmente, para evitar qualquer tipo de conflito ou colisão entre os dispositivos (Rufino, 2005).

Para Torres (2001), o IEEE padronizou os endereços MAC em um quadro com seis bytes, onde os três primeiros identificam o fabricante do dispositivo, e os três últimos são para o controlo do próprio fabricante, sendo necessário seu registo, o IEEE para poder receber sua OUI (Organizationally Unique Identifier). Um mesmo fabricante pode ter mais de um OUI, o que evita assim o problema de repetição dos números em caso de fabricação de dispositivos em grande escala.

A forma de prevenir uma entrada não autorizada, ou uma invasão em uma rede sem fios, é registar o endereço MAC (Media Access Control) de cada dispositivo da rede no controlador da rede, que pode ser um roteador, um ponto de acesso, entre outros. Esse controlador da rede, que só permitirá a entrada dos registados em sua base de dados, ignora outros que porventura possa tentar entrar em área da sua actuação (Rufino, 2005).

2.3.7 Autenticação

A autenticação é um método que garante a segurança de um sistema. Normalmente neste processo utiliza-se o nome de utilizador e uma chave secreta (senha), que guarda em uma base de dados o qual o autenticador fará a consulta para verificar se as informações estão certas, liberando assim o acesso às requisições solicitadas pelo elemento autenticado.

De acordo com Amaral (2004), existem duas maneiras de verificar se um utilizador wireless deseja acessar a rede, Autenticação de Sistema Fechado e Autenticação de Sistema Aberto.

Na autenticação de sistema aberto, um utilizador é autenticado mesmo se ele simplesmente responder com uma string vazia para o SSID (service set identifier), esta autenticação é conhecida como NULL Authentication. Com o segundo método, Autenticação de Sistema Fechado, utilizador wireless precisa responder obrigatoriamente com o SSID actual da rede wireless. O que significa que a cada utilizador é permitido o acesso se ele responder com a string correcta de 0 a 32 bytes, identificando o BSS da rede wireless.

2.3.8 RADIUS

O RADIUS é um protocolo de controlo de acessos que autentica e autoriza o acesso de utilizadores a redes. Este protocolo usa um cenário de cliente-servidor em que o cliente, designado de NAS (Network Access Server) envia pedidos de autenticação dos utilizadores e o servidor responde. As respostas do servidor poderão ser em forma de desafios, de aceitação ou rejeição do utilizador. O RADIUS é muito utilizado por fornecedores de acesso à Internet, bem como por organizações que pretendam um sistema de autenticação centralizado para autenticar o acesso à rede e aos seus recursos. O RADIUS apresenta ainda a vantagem de poder juntar informação referente à troca de dados e sessões de cada utilizador, a que se chama de contabilização. (Martins 2003),

Segundo Martins (2003), Contabilização é outro processo da norma AAA e que tem como funcionalidade guardar informação dos recursos acedidos por cada utilizador. Entre a informação guardada pode estar a quantidade de tempo que o utilizador utilizou o recurso, a quantidade de dados que foram trocados com o utilizador, o número de sessões do utilizador, entre outras. A contabilização pode ser usada para controlo de autorização, facturação por parte dos fornecedores de Internet, análises de ameaças, utilização de recursos, entre outros.

2.3.8.1 *Limitações do RADIUS*

Para Antunes (2009), Existem várias limitações na utilização do RADIUS:

- A segurança de uma rede está dependente da configuração usada. Por exemplo, numa configuração que possua vários servidores a funcionar como proxy, todos os nós devem processar e reencaminhar os dados no pedido. Devido ao modelo hop-by-hop do RADIUS, isto significa que dados, como certificados e palavras passe, estarão disponíveis em todos os nós o que ameaça a segurança da rede.

- O facto de os servidores RADIUS processarem cada pedido independentemente e, por isso, não relacionarem os pedidos do mesmo cliente não associando um estado a este complica as soluções de gestão de recursos e sessões dado que não existe uma sessão, isto é, uma conexão activa entre o cliente e o servidor.

2.3.8.2 *Descrição do Funcionamento do RADIUS*

O protocolo RADIUS baseia-se no modelo cliente/servidor, tendo de um lado o cliente ou o NAS (Network Access Server) que, embora seja uma gateway que controla o acesso à rede, possui uma componente que funciona como cliente, e do outro o servidor. O utilizador, o NAS e o servidor trocam mensagens entre si quando o utilizador se pretende autenticar para utilizar um determinado recurso da rede.
Uma mensagem RADIUS consiste num pacote UDP com um cabeçalho RADIUS contendo o tipo de mensagem e podendo ainda ter, ou não, alguns atributos associados à mensagem.
Cada atributo RADIUS especifica uma parte de informação sobre a tentativa de ligação. Por exemplo, existem atributos RADIUS para o nome de utilizador, palavra passe do utilizador, tipo de serviço pedido pelo utilizador e o endereço IP do cliente de acesso. Os atributos RADIUS são utilizados para transmitir informações entre clientes RADIUS, proxies RADIUS e servidores de RADIUS.(Antunes, 2009)

2.3.9 SSID

Para Nóbrega et al (S/D), SSID (Service Set identifier) é um conjunto de códigos alfanuméricos que identifica os computadores e os pontos de acesso da rede. Esses códigos são colocados pelos fabricantes e são fáceis de descobrir, pois cada um deles tem um padrão numérico de senha facilmente encontrado em manuais e na Internet.

Com esta opção activada, qualquer máquina que esteja situada dentro do sinal emitido por um AP poderá conectar-se à rede, sem saber previamente o código. O problema é que qualquer aparelho que esteja dentro da faixa pode ter acesso à rede, ficando fácil a qualquer pessoa invadir o sistema. Porém, para maior segurança da rede, recomenda-se ocultar o SSID e impedir que este seja exposto por broadcast.[4]

[4] http://www.uepb.edu.br/dmec/uepb/rev_eletric/artigoolavoigorhp.pdf acessado em 09/09/2009

2.4. Riscos e Vulnerabilidade de Rede Wireless

Para Amaral (2004), as fragilidades das redes de computadores, tanto as redes cabeadas como as redes sem fios, são inumeras e entre elas podemos destacar que:

- As características de segurança normalmente não são utilizadas
- As chaves de criptografia são partilhadas
- As chaves de criptografia são pequenas
- A RC4 tem uma chave fraca e é utilizado inapropriadamente no WEP
- A integridade do pacote é fraca
- Não ocorre autenticação do utilizador
- A Autenticação não é habilitada, somente uma verificação de SSID é feita
- A autenticação do dispositivo é muito simples

2.5. Segurança Física

Segundo (Silva, 2005) " … *Segurança física consiste na aplicação de barreiras físicas e procedimentos de controlo, como medidas de prevenção e contra medidas perante ameaças aos recursos e informação confidencial. Refere-se aos procedimentos de controlo e aos mecanismos de segurança dentro e em volta do Centro de Processamento de Dados, assim como os meios de acesso remoto implementados para proteger o hardware e os meios de armazenamento de dados ...* "

2.6. Localização do acess point

Segundo Guiar (2005), a qualidade e a segurança da rede estão directamente ligadas à localização do APs de uma rede sem fios dentro de uma pequena empresa, universidade, organização, ou até mesmo no meio doméstico. Dispositivos wireless como os APs devem ser localizados o mais alto possível dentro de um ambiente para reduzir a interferência e perda de sinal devido a barreiras mortais para o sinal de rádio como plantas, arvores, paredes de concreto e reservatórios de água. Alguns dispositivos Wireless já vêm com antenas ligadas a cabos longos para permitir melhor posicionamento das mesmas.

Capítulo 3: O caso da Universidade de Cabo Verde

3.1 Enquadramento

A segurança na rede sem fios constitui, actualmente, um dos aspectos mais importantes na questão do acesso por parte dos utilizadores da Universidade de Cabo Verde.

Durante os seus dois anos de vida, a rede da Uni-CV não dispunha de um sistema de segurança na sua rede sem fios, podendo qualquer pessoa a ela aceder, sem qualquer controlo ou permissão.

Em virtude dos constrangimentos que tal situação acarreta, nomeadamente no envio de vírus através da rede e na execução de pesquisas não autorizadas, entrar no servidor, entre outros, a Universidade teve a necessidade de criar um sistema de segurança na sua rede wireless.

Este projecto tem como objectivo principal melhorar a segurança wireless no acesso dos utilizadores à rede da Universidade de Cabo Verde - campus palmarejo.

3.2 Apresentação da Universidade de Cabo Verde

Para Lopes (2007), logo a seguir à Independência Nacional, em 1975, Cabo Verde enfrentou uma drástica crise de professores nacionais para a docência nos liceus da Praia. Paralelamente, assistia-se a uma expansão da procura do ensino secundário que se deveu, em grande parte, não só à expansão do Ensino Primário obrigatório, como à expansão do Ciclo Preparatório verificada nos últimos anos da gestão colonial.

O cenário de carência de docentes levou o primeiro Governo de Cabo Verde a recorrer à cooperação portuguesa, que se prontificou em enviar professores para as mais diversas disciplinas do currículo do secundário.

A solução pela via da cooperação mostrou-se insustentável: a disponibilidade de alojamento e demais condições de acolhimento, o crescimento das necessidades do aumento de número de cooperantes, aliado à crescente demanda do ensino secundário inviabilizou a cooperação.

Em 1979, atendendo a propostas de alguns técnicos da Universidade de Coimbra, o Ministério da Educação criou o Curso de formação de Professores (CFP) com o objectivo de formar professores do Ensino Secundário no domínios de: Língua Portuguesa, Ciências Histórico-Naturais, Física, Matemática. O CFP conferia o grau de bacharelato com a duração de três anos lectivos.

À data, a docência era assegurada por professores cooperantes em tempo parcial, sendo o quadro docente a tempo inteiro formado por uma professora que exercia em simultâneo a função de Directora Adjunto.

O CFP contou com o apoio directo de Universidades Portuguesas, como a Universidade de Coimbra e a de Lisboa, que se prontificaram a enviar docentes. Estabeleceram com o CFP protocolos de reconhecimento para efeito de finalização da licenciatura em Portugal. Posteriormente, este protocolo foi alargado a Universidades Públicas portuguesas.

Registe-se que todos os formandos que se deslocaram a Portugal completaram a formação com êxito.

O primeiro grupo de formandos que saiu do CFP, entrou no mercado de trabalho no ano lectivo de 1982/83. O CFP funcionou nas instalações do Liceu Domingos Ramos, embora

com secretaria própria. Em 1985, o CFP muda-se para o Parque 5 de Julho e, no mesmo ano, foram abertos novos cursos, a saber: bacharelato em História e mais tarde o bacharelato em Filosofia (Nesta data o quadro de docentes a tempo inteiro aumentou para três professores).

Em 1988/89, considerando a precariedade das instalações do Parque 5 de Julho, o aumento progressivo de alunos e a carência de espaço para funcionar laboratórios, secretaria, centros e bibliotecas, o CFP mudou de instalações para a "Escola Grande", no Plateau. Isso com base no espírito de criação de uma estrutura de formação de nível superior, especialmente expresso na Lei de Bases do Sistema Educativo.

Em 1990, assiste-se à mudança do CFP para a Escola de Formação de Professores do Ensino Secundário – EFPES. O leque de Cursos de saída é alargado para os Cursos de Língua Inglesa e Francesa.

O Governo da segunda República criou a Comissão Instaladora do Ensino Superior - CIES, que tutelou a EFPES e o Curso Propedêutico, transformado em Ano Zero. Ainda era incumbência da CIES a criação da Universidade de Cabo Verde

No entanto, a dinâmica do processo, as contribuições e as solicitações dos docentes para a clarificação dos objectivos da Escola, que então atravessava um período crítico, levou o Ministério da Educação a transformar a EFPES no Instituto Superior de Educação (ISE), com Estatuto próprio e nova tabela indiciária e salarial do pessoal docente.

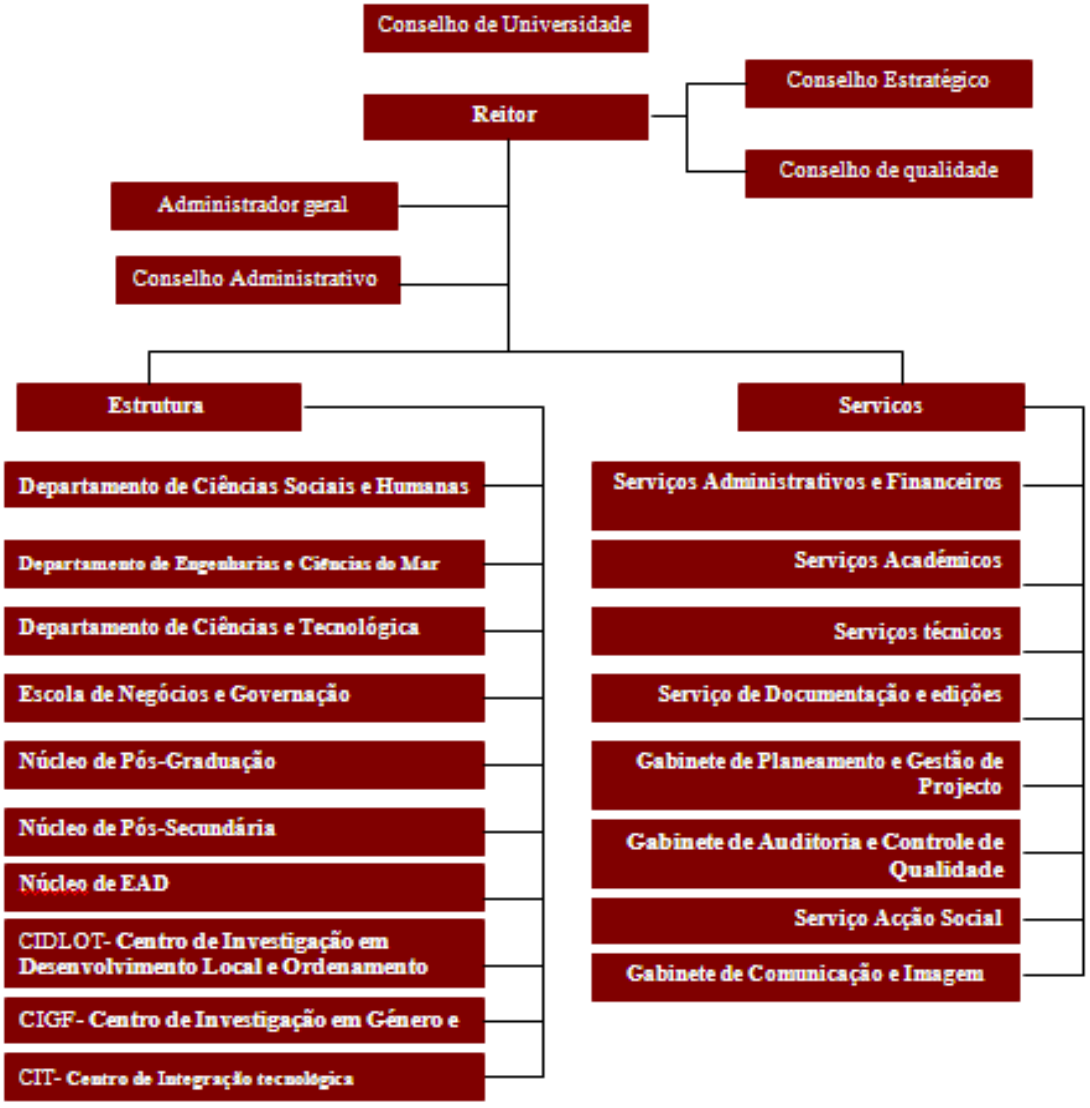
Desde a sua criação, o ISE contou com estatuto próprio cujos princípios fundamentais eram a autonomia científica, pedagógica, patrimonial, administrativa e financeira. Reuniões periódicas do Conselho Cientifico e Regulamento dos Departamentos.

No ano Lectivo 2002/2003 o ISE muda-se para o seu actual edifício situado no Palmarejo.

No entanto, após esse processo, que decorreu durante algum tempo, veio o período de transição em que o Instituto Superior de Educação passou a ser denominado de Universidade de Cabo Verde (Uni-CV). Hoje esta Instituição engloba outras instituições de ensino, isto significa que a nova instituição já tem outros propósitos em relação a ensino/aprendizagem.

3.3 Organograma da Universidade de Cabo Verde

Na figura em abaixo, apresenta-se o organograma da instituição.



Figuras 1: Organograma da Uni-CV (Fonte: Lopes/Uni-CV)

3.4 Planeamento do estágio

Para a concretização deste projecto, o trabalho foi realizado pelas seguintes fases:

- Pesquisa Bibliográfica
- Levantamentos dos equipamentos informáticos
- Desenho lógico do sistema
- Desenho de Domínio da Universidade
- Desenho da Infra-estrutura da rede

Instalação de Windows server 2003

- Preparação da instalação
- Inicio do Instalação
- Instalação do active directory
- Criação do Utilizador
- Adicionar o utilizador ao grupo

Integração de servidor RADIUS no Windows server 2003

- Instalação da CA (Certificate Services)
- Instalação de IAS (Internet Authentication serveces)
- Configuração do RADIUS
- Configuração do acess Point
- Configuração do Cliente Windows XP

3.5 Apresentação do estágio

O projecto desenvolvido no estágio, que ora se apresenta, aborda a tema Segurança wireless na Universidade de Cabo Verde, cujos principais objectivos são: **instalação do servidor** e **active directory,** que serve para armazenamento de todos os dados da Universidade de Cabo Verde, instalação do **IAS -** que é uma estrutura de autenticação central disponibilizada pelos serviços de directória do Windows - , instalação de Certificate Sevices e a instalação do sevidor **RADIUS,** que é a parte mais importante, porque **é** dentro do servidor RADIUS que estão todas as contas dos utilizadores para autenticar na rede wireless da Universidade.

Com um número de utilizadores incontrolável no uso da rede wireless da Universidade, houve necessidade de se criar as condições necessárias, de forma de ter maior controlo da utilização, garantindo um mecanismo de controlo e segurança de todos os utilizadores da rede wireless da Universidade de Cabo Verde.

3.6 Pré-requisitos

- Servidor com Windows servidor 2003 e AD (domain controller e Pelo menos SP1)
- Um ou mais Clientes Windows XP com placas Wireless Instalada (SP1)
- AP Com Suporte 802.11i e 802.1x

3.7 Ferramentas Utilizadas

As Ferramentas utilizadas para realização deste trabalho são:

- Windows Server 2003
- EDrawNetDiagram.exe
- O Microsoft Office visio 2007 -

3.7.1 Descrição do Windows Server 2003

O Windows Server 2003 é o mais rápido, confiável e seguro sistema operacional de servidor Windows já oferecido pela Microsoft. O Windows Server 2003 proporciona confiabilidade da seguinte forma:

- Fornece uma infra-estrutura de TI que oferece um valor fundamental: confiabilidade aprimorada, melhor disponibilidade e maior escalabilidade. Incluindo uma plataforma de aplicativo com a funcionalidade tradicional de servidor de aplicativo integrado no topo dos extensos recursos do sistema operacional.
  Integrando uma infra-estrutura de operador de informações que ajuda a manter as informações comerciais seguras e acessíveis.

- O Windows Server 2003 oferece as ferramentas que simplificam a implantação, gestão e a administração e aumenta a produtividade.

3.7.2 Função de Windows server.

O Windows Server 2003 é um sistema operativo que controla vários funções do servidor, de acordo com as suas necessidades, de forma centralizada ou distribuída. Algumas dessas funções do servidor incluem:

- Servidor de arquivos e impressão.
- Servidor Web e serviços de aplicativos da Web.
- Servidor de email.
- Servidor de terminal.
- Servidor de acesso remoto e rede virtual privada (VPN)
- Serviços de directório, sistema de nomes de domínio (DNS)
- Servidor de protocolo DHCP e serviço de registo na Internet do Windows (WINS).

3.7.3 Descrição do EDrawNetDiagram.exe

EDraw Network Diagrammer é um software de diagramas profissional da rede, com vários exemplos e modelos. Fácil de fazer desenho físico, lógico e diagramas de arquitectura de rede, tem um conjunto modelo de rede e as formas de equipamento informático, como por exemplo computadores, dispositivos de rede mais utilizados, conectores de rede, diagrama de design, criação de diagramas de rede precisa e documentação para ser usado em seu projecto de diagrama de rede.

3.8 Planeamento de Actividades do Estágios

Um planeamento das actividades ajuda a manter uma ideia dos objectivos e das tarefas que ainda tem que fazer para atingir os objectivos.
O estágio concentra-se inicialmente na elaboração do tema e pesquisa bibliográfica, e apresenta todas as actividades abordadas durante a concepção do estágio.

3.8.1 Pesquisa Bibliográfica

Na primeira e segunda semana do estágio, demos início à Pesquisa Bibliográfica. Foi efectuada uma pesquisa bibliográfica onde o objectivo principal era fazer recolha de informação para saber como implementar segurança wireless no Campus de Palmarejo da Universidade de Cabo Verde.

Depois da pesquisa bibliográfica, fizemos um levantamentos de todos os equipamentos informáticos e do número de alunos existente. Elaboramos o desenho lógico de sistema e da infra-estrutura da rede para explicar o que foi feito durante o estágio

3.9 Desenho lógico do sistema

O desenho lógico apresenta reais vantagens quando integrado com a Active Directory, ou seja com a estrutura de autenticação central disponibilizada pelos serviços do Windows server 2003.

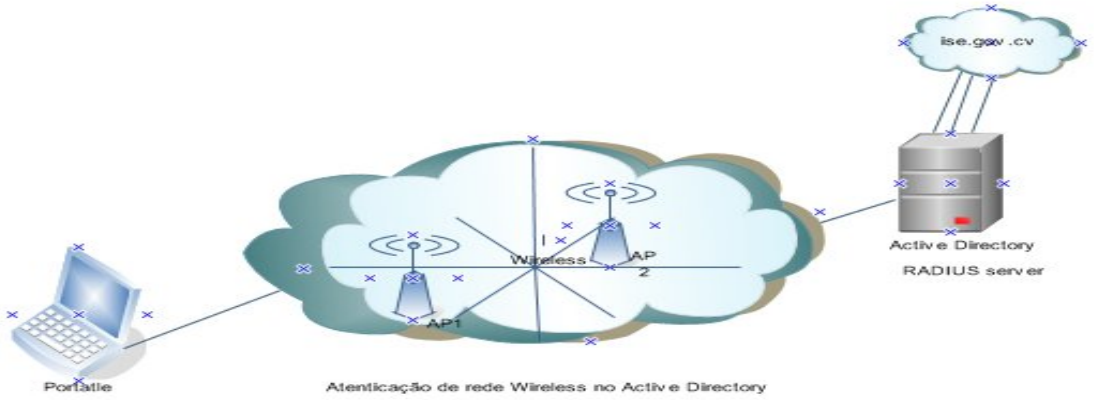


Figura 2:autenticação de rede wireless no active directory

Descrição do desenho

O desenho acima sintetiza todo o trabalho desenvolvido na criação e estruturação do acesso dos utilizadores à rede wireless com integração do active directory.

Este desenho arquitectural tem como objectivo principal desenhar a estruturação do acesso à rede wireless, de modo a conseguir maior controlo dos utilizadores.

Assim, com esta estrutura será mais fácil fazer controlo de todos os utilizadores da Universidade de Cabo Verde – Campus do Palmarejo. Também permite maior segurança nos acessos a rede wireless, melhor comunicação entre os mesmos e uma maior rigidez no controlo de acesso.

No desenho existe o servidor RADIUS, dois acess point e um portatle. Apenas o utilizador que tem conta criada no active directory da Uni-CV- Campus de Palmarejo - tem acesso a rede wireless.

3.10 Infra-estruturas das TIC da Uni-CV

O *campus* da Universidade de Cabo Verde em estudo fica situado na cidade da Praia especificamente na zona do Palmarejo. É uma Universidade que já recebeu milhares de formandos e, é lógico, que com a evolução dos tempos esteja se preparando para o novo mundo da tecnologia, que é sem dúvida um motor do desenvolvimento não só do país, como também no ensino/aprendizagem.

Actualmente, a Universidade constitui uma estrutura mais unida com dois dos seus departamentos a funcionar no campus do Palmarejo, DCT e DCSH (depatamento de Cuiência e tecnologia e Departamento de Ciências Sociais e Humansa) responsabilizados por dois sector, e cumprindo a execução das diferentes tarefas a serem executadas no dia-a-dia da Instituição.

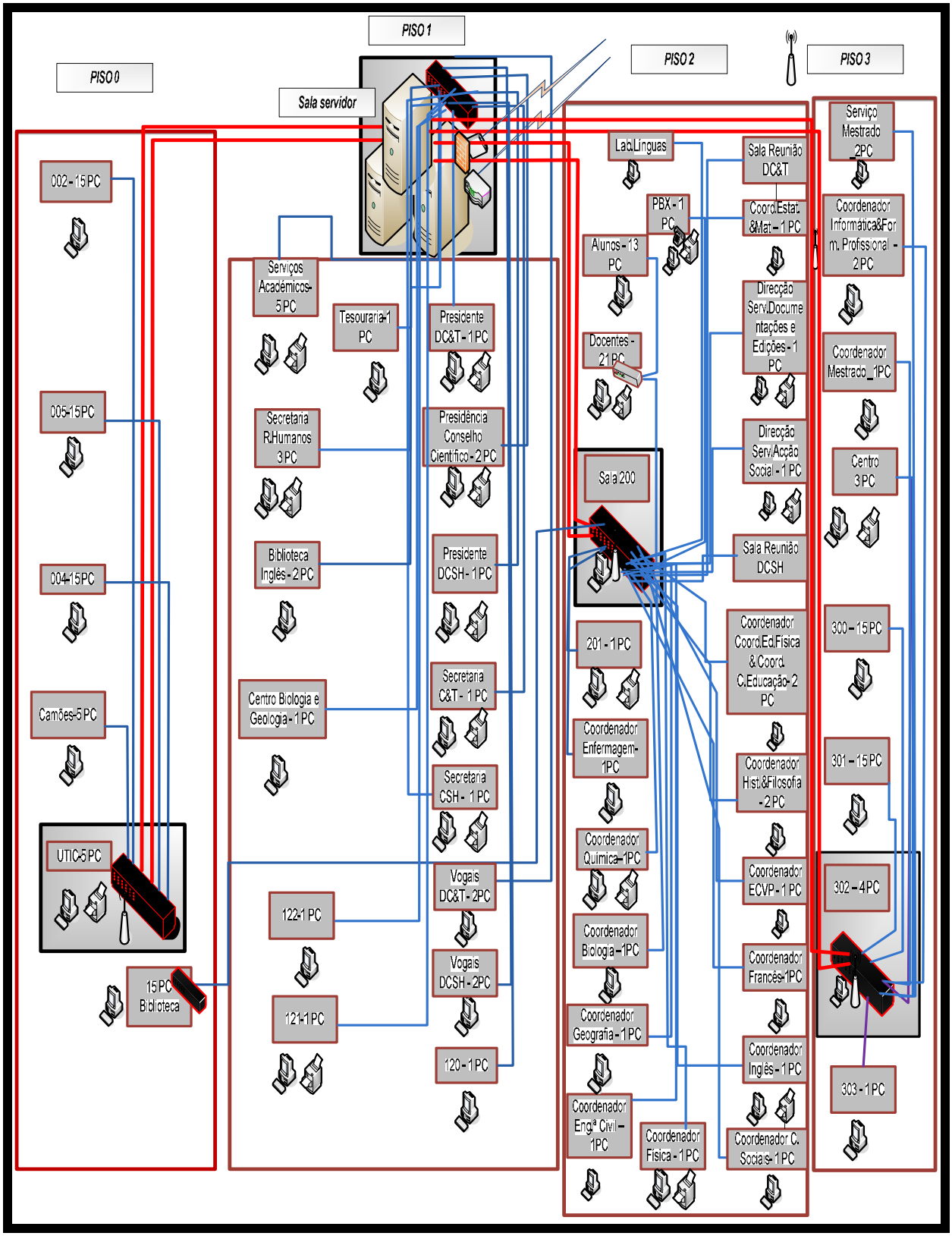
3.10.1 Números de computadores/impressoras

A Instituição está dotada de computadores, e muitos deles são bem recentes, permitindo assim trabalhar razoavelmente de modo a atingir os objectivos dos cursos e da própria Instituição. A instituição possui 274 computadores, todos ligados à rede, 11 impressoras também partilhadas pela rede.

3.10.2 Equipamentos de rede

Na rede da Universidade de Cabo Verde, campus do Palmarejo, todos os equipamentos necessários estão ligados para o funcionamento da própria rede. Existe na rede 12 Switches, 2 routers, um modem, 3 servidores, 24 réguas e 4 acess point.

Rede da Universidade de Cabo Verde Campus de Palmarejo

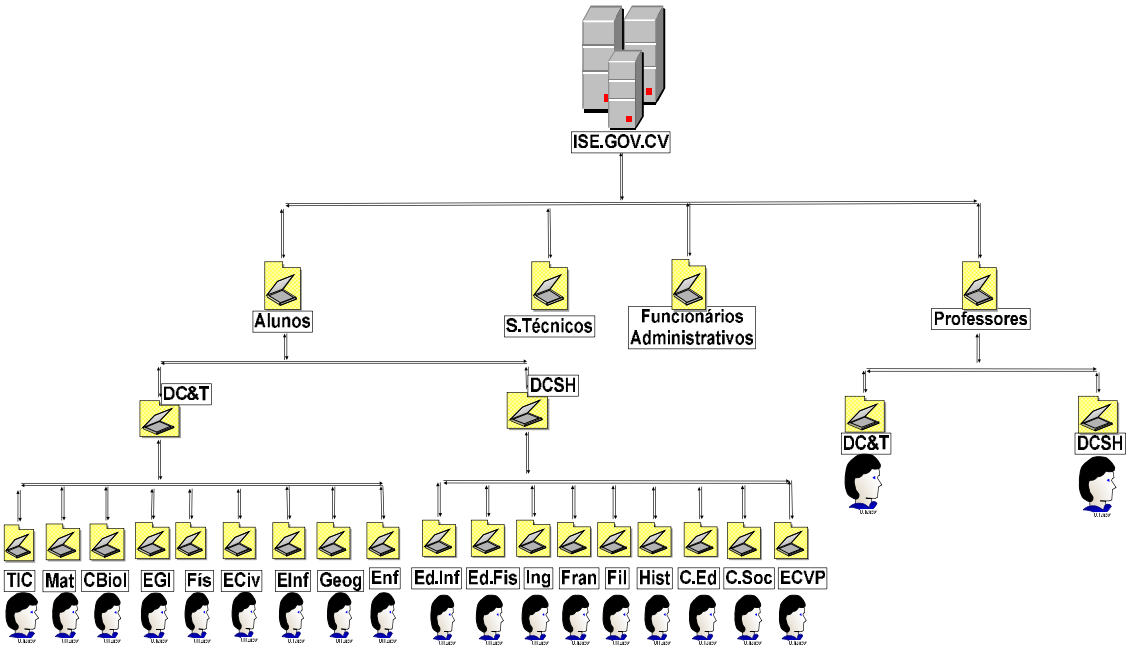


Figuras 3:Infra-estrutura da rede da Uni-CV

3.1.1 Instalação do Servidor na Uni-CV Campus Palmarejo

Na terceira semana do estágio, durante a qual deu-se início à instalação do servidor, configuração do servidor e Instalação do active directory e o seu desenho arquitectural do Active directory.

Desenho do Active Directory



Figuras 4:Desenho do Active Directory

O desenho acima, mostra o domínio no topo ise. gov.cv, e as unidades organizacionais. Este desenho tem como principal objectivo mostrar a estruturação e organização da distribuição dos recursos, de modo a conseguir uma maior racionalização dos recursos.

Com isso, será mais fácil fazer a partilha dos recursos e a definição de políticas em toda a organização. Ainda, permite maior segurança nos domínios criados, melhor comunicação entre os mesmos e um maior rigor no controlo de acesso.

Segundo Santos e Rosa (2002), a active directory é o serviço de directório utilizado em uma rede Windows 2003, sendo um serviço de directório, serve à nossa rede como um depósito central para armazenamento de informações dos utilizadores, como nomes, senhas, números de telefone e assim por diante, e permite que outros utilizadores autorizados da mesma rede tenham acesso a essas informações.

Alguns benefícios do *Active Directory*:

- Segurança da informação: O controlo do acesso pode ser definido quer ao nível de cada objecto, quer ao nível da sua propriedade;
- Administração baseada em políticas: permite determinar regras que restringem o acesso aos objectos do directório e aos recursos do domínio;
- Extensibilidade: representa a capacidade de introduzir novas classes de objectos e de criar e alterar os seus próprios atributos de objectos já existentes;
- Escalabilidade: consiste na capacidade de adicionar novos Controlador de Domínio, permitindo assim o aumento das capacidades da rede e uma mais eficaz distribuição dos recursos;

3.2 Criação Unidade organizacional

A Criação de Unidade Organizacional permite efectuar uma divisão de um domínio em diversas unidades que façam sentido na estrutura da rede da **Uni-CV,** e permite definir para cada uma delas políticas de grupo e esquema de segurança.

As permissões de acesso a rede wireless são baseadas nesses grupos.
O objectivo é facilitar em muito a administração, pois definem-se uma única vez as permissões para os grupos e utilizadores.
Será criado um grupo chamado acess point, que contem todos os utilizadores que têm acesso a rede wireless da universidade.

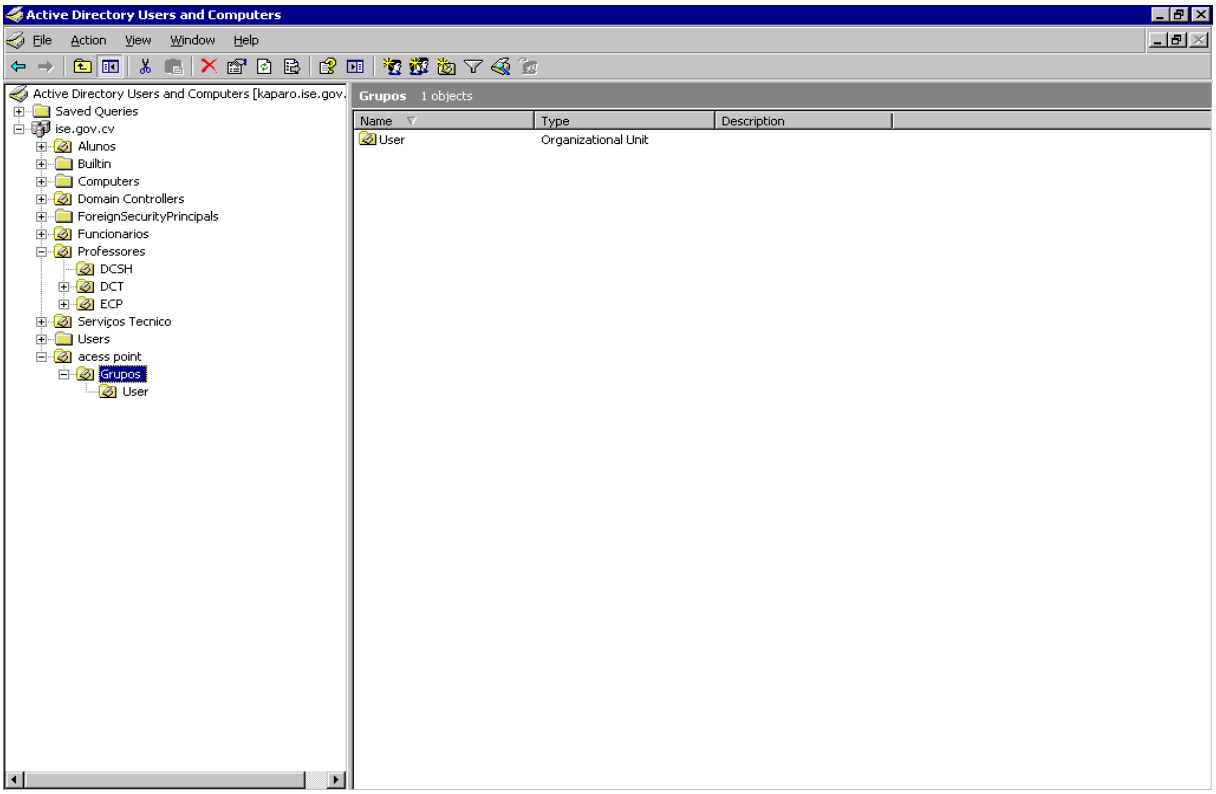
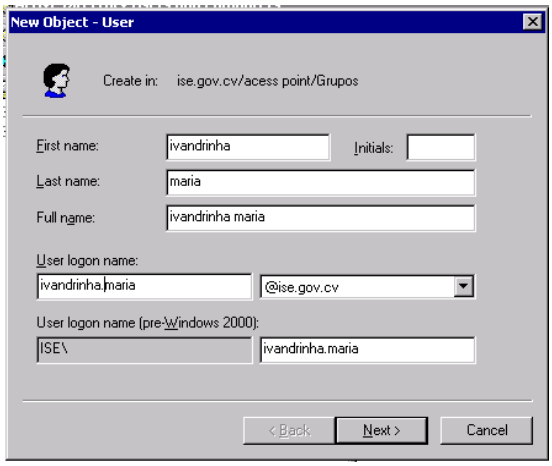


Figura 5: Acesso o OU Grupos

É importante criar contas porque são registos de identificação e configuração de utilizadores autorizados.

Como sabemos, conta é um conjunto de dados que identificam e caracterizam uma entidade que deve ser reconhecida por um domínio. Essa entidade pode ser uma pessoa ou um grupo de pessoas.

A figura em baixo mostra inserção do utilizador mais detalhes ver no Manual



Figuras 6: Inserção de Utilizador

3.3 Integração de servidor Radius no Windows Server 2003

Na sétima semana do estágio, em execução com o Plano de Actividades, sucedeu-se a integração de servidor RADIUS no Windows server 2003.

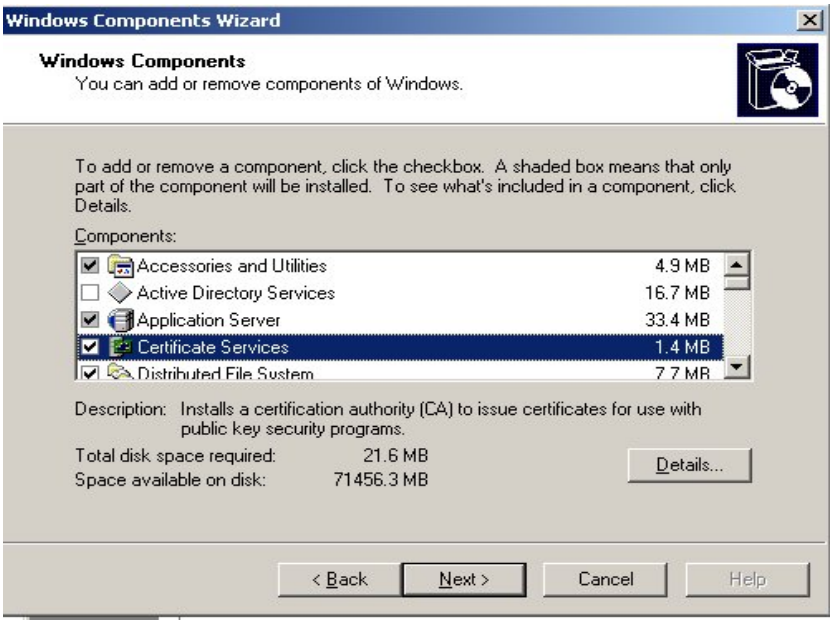
É no servidor RADIUS, que todas as contas dos utilizadores autenticados estão armazenadas, para ter o acesso à rede wireless da Universidade e permitir definir para cada uma delas políticas de grupo e esquema de segurança.

O acesso à rede wireless é baseado nessa conta de utilizadores também e nesse Servidor é configurado o acees point para que os utilizadores possam ter acesso wireless através do servidor RADIUS.

3.3.1 Instalação da CA (Certificate Services ou authority)

De início foi criada uma autoridade certificadora (AC) com um nome CAtest. É através dela que todos os certificados digitais são emitidos, bem como autoridades certificadoras intermediárias para melhor organizar os certificados. Os utilizadores da rede da Universidade devem requisitar seus próprios certificados .

A Figura que se segue mostra a instalação do Certificate Services. Mais detalhes podem ser consultados no Manual de Configuração em anexo.

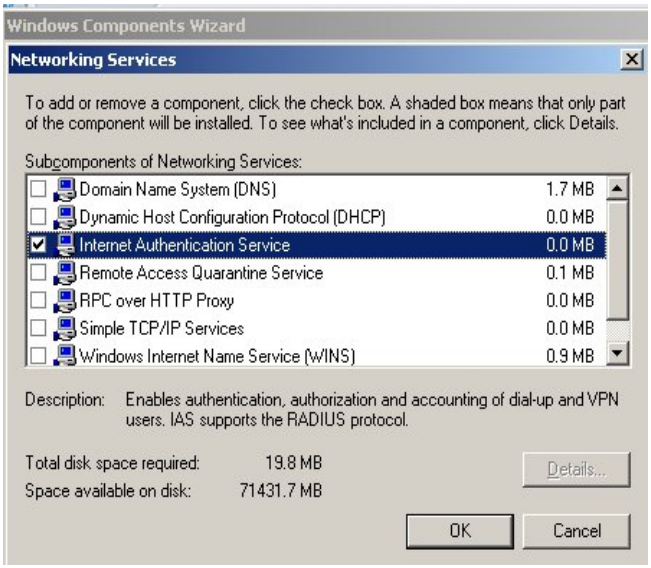


Figuras 7: Instalação do Certificate Services

3.3.2 Instalação de IAS (Internet Authentication Services)

É importante instalar o IAS porque apresenta vantagens reais quando integrado com a ActiveDirectory, ou seja, com a estrutura de autenticação central disponibilizada pelos serviços de directoria do Windows.

A figura que se segue mostra a instalação da Internet Autentication Server. Mais detalhes podem ser consultados no Manual de Configuração em anexo.



Figuras 8: Internet Autentication Service

3.3.3 O processo de Autenticação e Autorização RADIUS

O RADIUS é um protocolo utilizado para disponibilizar acesso a redes. Inicialmente foi desenvolvido para uso em serviços de acesso discado.

Actualmente, é também implementado em pontos de acesso sem fio e outros tipos de dispositivos que permitem acesso autenticado a redes de computadores.

O RADIUS foi concebido para centralizar as actividades de Autenticação, Autorização e

Contabilização. O processo de autenticação funciona da seguinte maneira: um host faz uma requisição de acesso a um cliente RADIUS. Este cliente requisita os dados e os parâmetros da conexão ao host de origem e os envia na forma de uma mensagem RADIUS, ao servidor. Este servidor observa os dados enviados e autentica e autoriza a requisição do cliente RADIUS. Sendo o acesso autorizado ou negado, uma mensagem é retornada ao cliente. No caso de acesso autorizado, o cliente libera o acesso à rede ao computador que fez a requisição de acesso.

A figura que se seque mostra o processo de Autenticação e Autorização RADIUS

Figuras 9: o processo de Autenticação e Autorização RAIUS

3.3.4 Configuração do Acess Point

O Access Point é um equipamento armado com um rádio transmissor/receptor, que actua como um bridge transparente, permitindo a comunicação entre dispositivo wireless e uma estrutura de rede concertada, com taxas de até 11 Mbps. Ainda pode ser utilizado para interligar duas redes remotas, através de um link de rádio, diminuindo bastante os custos de comunicação e viabilizando a integração dos sistemas administrativos devido à grande largura de banda suportada. Concentra todo o tráfego da rede wireless além das conexões oriundas dos clientes. Possui um identificador que identifica a rede chamado SSID. (Lopes et al 2008)

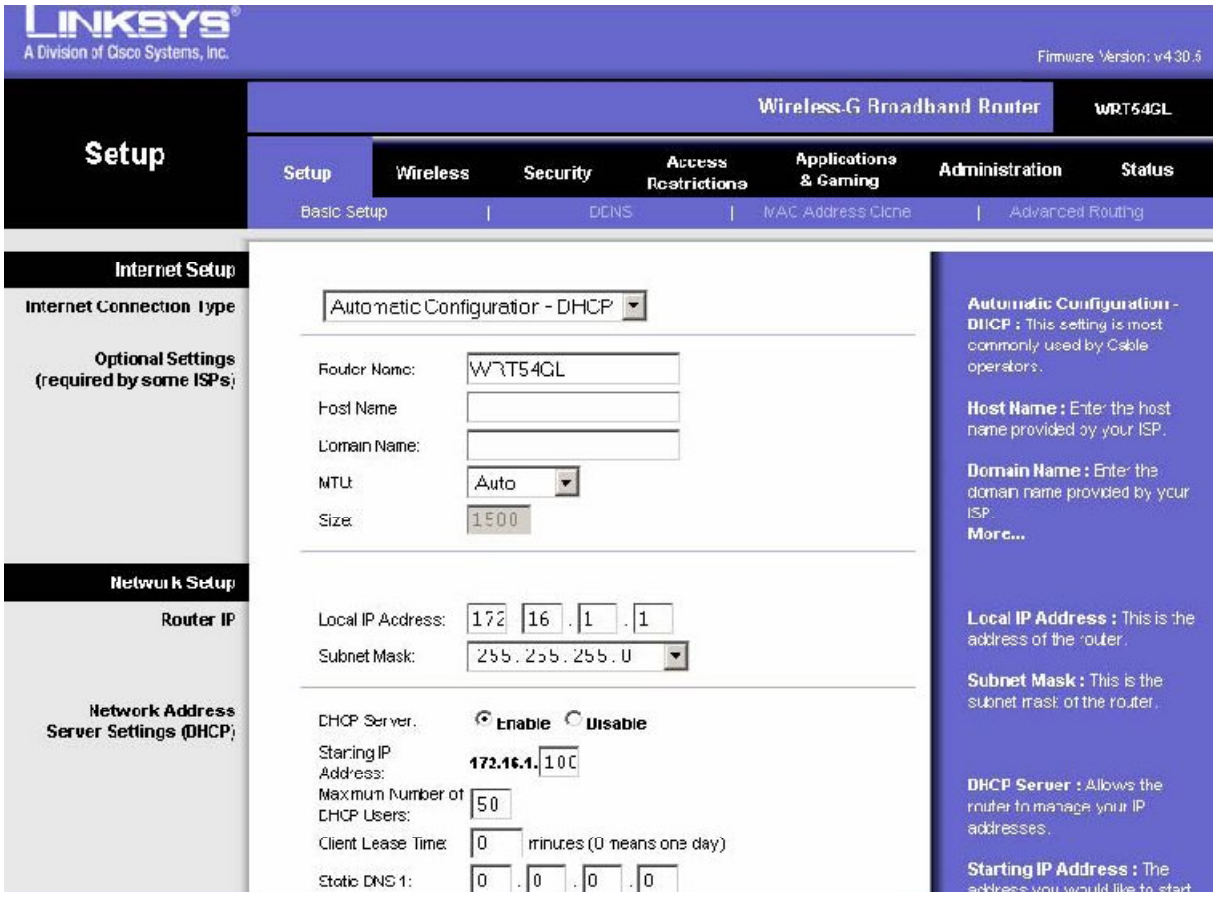
Por último, para completar as actividade do estágio, fez-se a configuração do acess point.

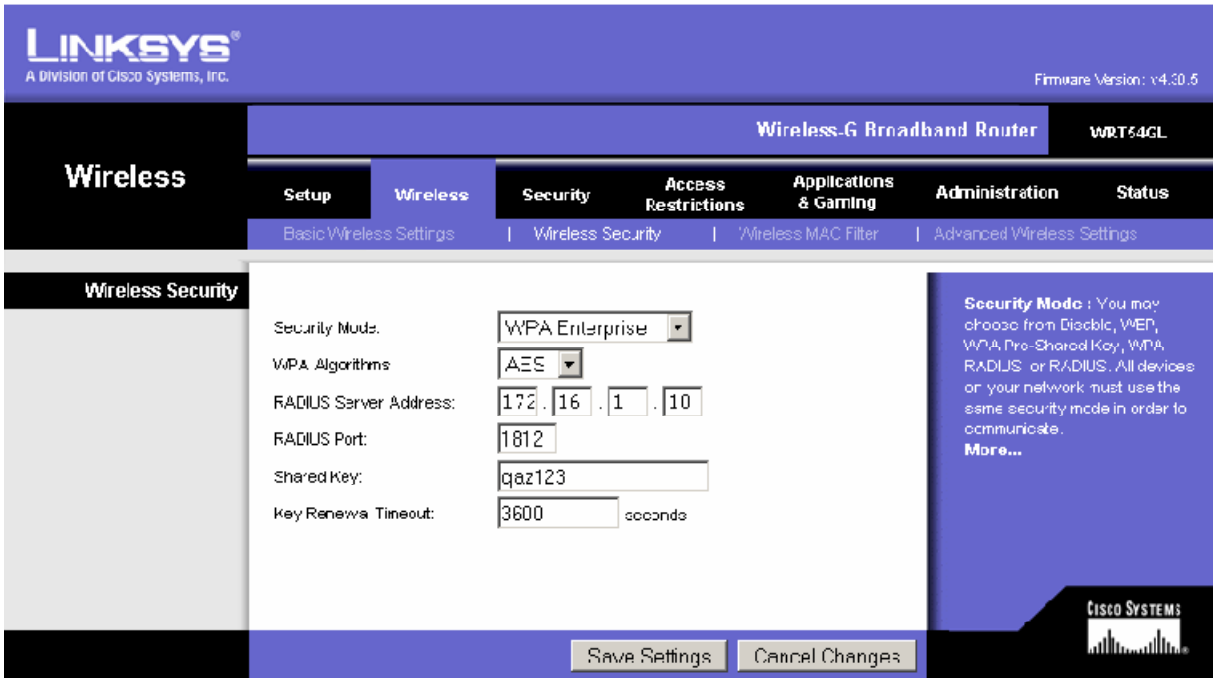
Com o servidor Radius configurado é necessário que o access point também esteja configurado para poder corresponder ao pedido de autenticação ao servidor. Portanto, para configurar o access point é necessário o acesso ao mesmo. Normalmente a interface de configuração é via browser, digita-se o endereço ip do access point.

Nos tópicos em baixo mostramos como configurar o acess point

- Na aba de segurança escolha a opção WAP Enterprise
- Define a encriptação com o método AES
- Insira o IP do Windows 2003 server (O Servidor RADIUS)
- Insira a chave que foi introduzida na IAS
- Server: W2k Radius IP
- Port : 80
- Radius secret : A mesma palavra que foi digitada no servidor Radius

Figura em baixo mostra configuração do acess point





Figuras 10:Configuração do acess Point

3.4 Configuração do Cliente Windows XP

Para configuração do cliente Windows XP deve-se seguir estas instruções:

- Aceda ao network connection através do painel de controlo
- Aceda as propriedades de wireless network connection
- Aceda a aba Wireless network e faça click em add
- Insira o SSID do AP
- Defina o tipo de autenticação para WAP2 e encriptação AES
- Faça Click na aba de autenticação
- Defina o EAP Type como protected EAP(PEAP)
- Faça click em propriedades,validate server deve estar activado
- Connect to these servers não deve estar activado
- Procure o Certificado Instalado na lista “Trusted root Certification Authoities “ e active-o
- Certifique-se que o método de autenticação esta definido como EAP-MSCHPv2
- Active o fast Reconnect
- Faça o login com um utilizador válido e lembre que este utilizador deverá ter acess permitido.

3.5 Considerações Finais

Para a restrição de acesso à rede sem fios utilizamos um servidor RADIUS com autenticação de uma CA, que obriga somente os utilizadores registados, que possuem acesso a rede, e desta forma torna-se possível a identificação e restrição dos acessos.

Durante todo o processo de avaliação, procurou-se buscar métodos seguros e envolvendo as melhores práticas recomendadas pelos fabricantes dos softwares já instalados na Universidade de Cabo Verde, Campus - Palmarejo.

Portanto, é perfeitamente viável a implementação do projecto, pois todos os obstáculos encontrados foram superados de forma eficiente e, consequentemente, tornando a rede da Universidade de Cabo Verde – Campus do Palmarejo mais segura e mantendo o foco principal para fins de pesquisas e crescimento intelectual dos que dela fazem uso.

Conclusão

A interacção com outro sistema situado remotamente, a necessidade dos utilizadores, exige cada vez mais das organizações a utilização das novas tecnologias e uma maior segurança, devido às ameaças que estas poderão sofrer por parte de acessos não autorizados. Tais acessos, podem trazer resultados desastrosos para as organizações. Mas como podemos minimizar esse factor de vulnerabilidade?

Uma das formas de minimizar esse risco é a integração de rede sem fios no servidor RADIUS e Windows Server 2003, ficando o acesso à rede sem fios feito Mediante a Autenticação integrado na active directory, nas redes organizacionais, porque esta permite garantir o acesso seguro às informações.

Portanto é possível fazer instalação do servidor RADUIS na Universidade de Cabo Verde, para ter mais segurança e controlo dos utilizadores, visto que a universidade possui um número elevado de utilizadores.

O estágio foi de grande valia para o enriquecimento, crescimento a nível profissional. A nível pessoal, a realização deste projecto permitiu alargar bastante os conhecimentos sobre as tecnologias utilizadas, bem como aumentar a capacidade para a comunicação de redes. Pela primeira vez tive a oportunidade de desenvolver um projecto e com muita valia para a universidade.

3.1 Limitações

Durante a realização do estágio, encontramos algumas dificuldades, que, geralmente, estão na realização de qualquer trabalho. Neste caso, as dificuldades centraram-se, logo no título do projecto, na configuração de RADIUS, por ser a primeira vez a fazer a instalação do servidor RADIUS, a instalação de IAS e CA.

Bibliografia

ABRAS, Gustavo (2002). *Wireless LAN* acessado em 1/09/2009

AGUIAR, Paulo (2005) *Segurança em rede Wi-Fi* acessado em 07/09/2009, Disponivel em http://www.ccet.unimontes.br/arquivos/monografias/73.pdf

ALBUQUERQUE, Alessandro (2008). *Artigo Científico: Estudo de Métodos de Protecção de Rede Wireless* acessado em 13/08/2009

AMARAL, B et al (2004) Segurança em rede Wireless 802.11 disponivel em ftp://ftp2.biblioteca.cbpf.br/pub/apub/2004/nt/nt_zip/nt00204.pdf acessado em 10/09/2009

ANTUNES, Victor. *Frontend Web 2.0 para Gestão de RADIUS.* Acessado em 3/11/2009

BRASIL, Marcelo (2004) *Redes Wireless: Flexibilidade Versus Vulnerabilidade* Disponível em http://wendell.cefetce.br/wendell/alunos/monogmarcelo.pdf acessado em 07/09/2009

Criptografia e CertificaçãoDiponivel em: http://www.training.com.br/lpmaia/pub_seg_cripto.htm acessado em 07/09/2009

GEMINES, Eder (2005). *Segurança de rede Wireless* acessado em 13/08/2009
http://www.malima.com.br/wifi/wifiArtigos.asp 18/08/2009

http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod170.mspx.17/08/2009

JÚNIOR, Alcides (2003) *Segurança em rede wireless* acessado em 07/09/2009 disponível em http://www.ppgia.pucpr.br/~jamhour/Download/pub/Outros/Monografia%20WLAN.pdf

KAMINSK, E.et al (2007). *Segurança e controle de Acesso acess point/Intenet* acessado em 13/08/2009

LEITE, Salatiel (2007). *Comunicação Wireless* acessado em 04/09/2009

LOPES, Marques (2007). *Panorama do ensino Superior em Cabo Verde* acessado em 1/09/2009

LOPES,B.et al (2008).*Auditoria de Redes* acessado em 18/08/2009

MARTINS, Marcelo (2003) *Protegendo redes Wireless 802.11b* disponível em http://www.projetoderedes.com.br/apostilas/apostilas_seguranca.php acessado em 08/09/2009

MEDEIROS, Carlos (2001). "*Segurança da Informação Implantação de Medidas e Ferramentas de Segurança da Informação"*. Disponível em http://www.linuxsecurity.com.br/info/general/TCE_Seguranca_da_Informacao.pdf, acessado em 04/09/2009

Microsof *Arqutectura da Solução LAN Sem Fio Protegido* Disponivel em http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod169.mspx 17/08/2009

NÓBREGA,O,etal, *Segurança em rede Wireless* disponível em http://www.uepb.edu.br/dmec/uepb/rev_eletric/artigoolavoigorhp.pdf acessado em 09/09/2009

ONO, Edson. (2004). *"Implementação de rede wireless de alta velocidade"*. Disponível em http://www.lisha.ufsc.br/~guto/teaching/theses/ono.pdf, acessado em 04/09/2009.

PAULO, Márcio redes Wireless (2008) Disponivel http://redeswirelessdf.blogspot.com/2008/05/vantagens-e-desvantagens-das-redes-sem.html.Em 14/08/2009

RUFINO, Nelson (2005) *Segurança em Redes Sem Fio*. Acessado em 10/09/2009

SANTOS, S.; Rosa, A. *Windows Server 2003*. FCA - Editora de Informática Ltda, 2002.Acessado em 18/08/2009

SILVA, Artur (S/D), *Redes Wireless* http://jsilva.tecnociencia.jor.br acessado em 22/09/2009

SILVA, Elcilina (2005), *Perfil de Utilizadores em Redes Locais,* Universidade Jean Piaget de Cabo Verde. Em 3/10/2009

SOUSA, Lindeberg (2002), *Redes de Computadores-dados,voz Imagen*,6º Edicão, editora Erica acessado em 11/09/2009

TOMÈ, Edgar (2003). *Artigo Científico: Wireless* acessado em 11/08/2009

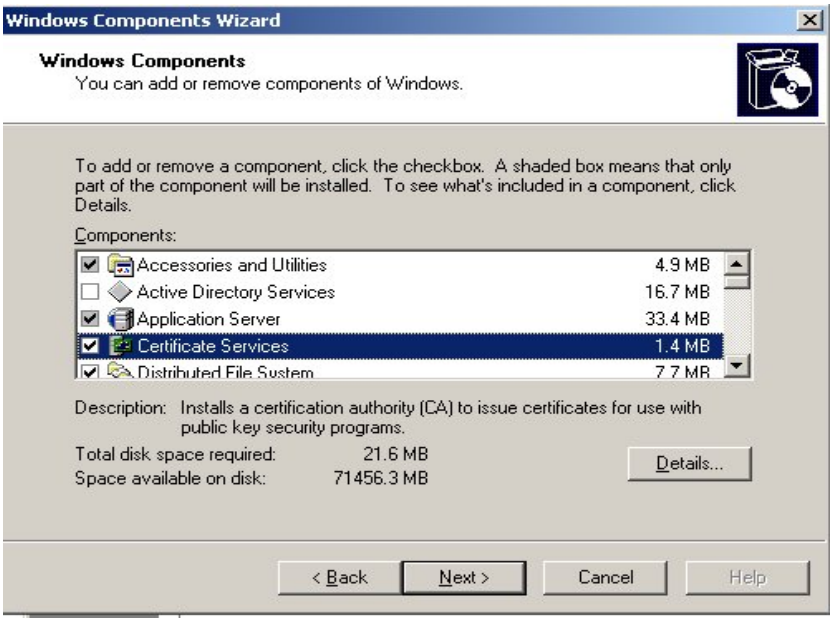
TORRES, Gabriel. *Redes de Computadores, Curso Completo*. Editora Axcel Books, 2001 acessado em 10/09/2009.

Wireless IP Tipo de ligação a rede sem fios Disponivel em http://www.wirelessip.com.br/wirelessip/tipos_ligacao 18/08/2009

A Manual de configuração

A.1 Instalação da CA (serviços de certificados)

Para adicionar uma CA em um servidor Microsoft Windows 2003 Server utilize o "Windows Components Wizard". Para localizar acesse o "Control Panel" > "Add or Remove Programs" e então escolha "Windows Components" em seguida selecione "Certificate Services" e clique no botão "Next", conforme a e figura em baixo.

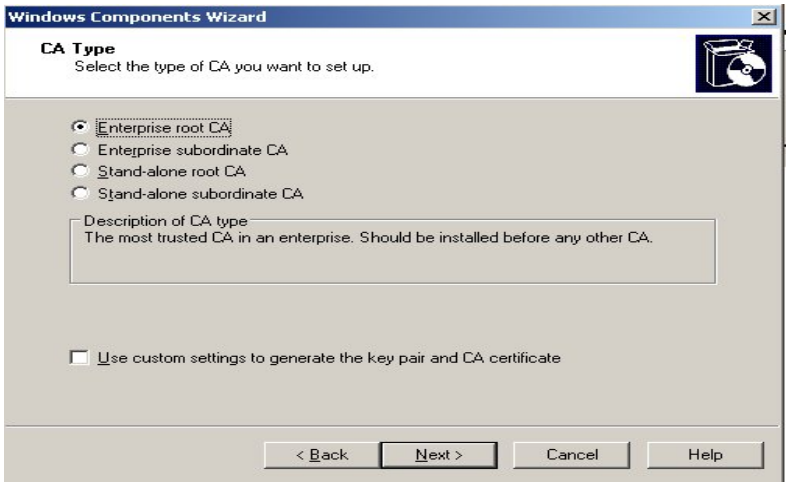


Instalação de serviço de certificado

Ao instalar um serviço de certificados aparece informação que não pode alterar o nome do servidor, também não pode ser removido do domínio. Clique “Yes” para prosseguir. Caso seja necessário alterar o nome do servidor ou remove-lo do domínio será necessário remover e instalar o serviço de certificado novamente, com isso todos os certificados emitidos serão removidos da CA, perde a sua validade.

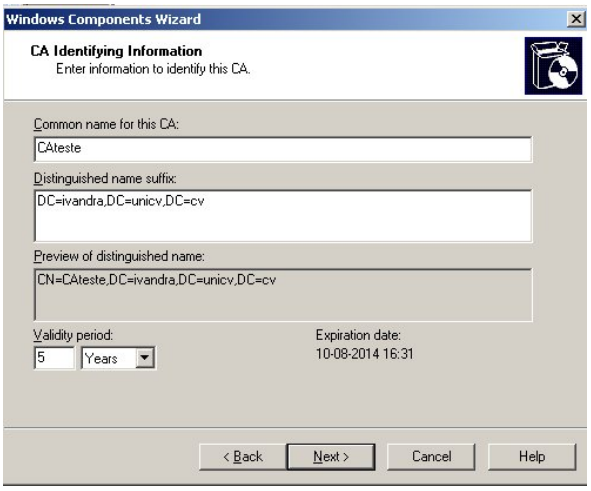
:Aviso da Instalação de um Serviço de Certificados

Em seguida delas defini o tipo da autoridade do certificado, utiliza a autoridade de certificação raiz corporativa, essa opção requer o Active Directory instalado no computador. Selecione o tipo “Enterprise root CA” e clique no botão “Next” conforme figura em baixo.



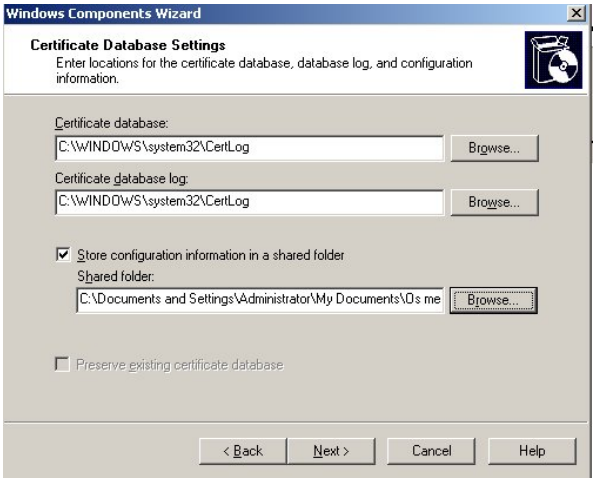
Seleccionando o tipo de autenticação de Certificação

O próximo passo é a definição do nome da CA e demais dados de identificação do certificado conforme figura em baixo. A descrição irá aparecer no certificado.



Informações de Identificação do Certificado.

Depois informa o local de armazenamento dos dados, estas informações já esta preenchidas, apenas dê um clique no botão "Next" para prossiguir com a instalação.

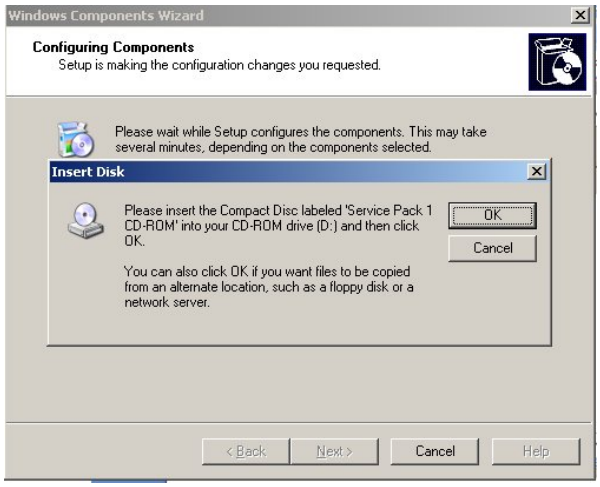


Local de armazenamento de Dados.

Para Gestão de emissão de certificados foi utilizado um serviço de HTTP, a instalação verificou se existe um servidor de HTTP instalado no servidor, caso não tenha é necessário instalar, depois demora nos serviços do HTTP para a criação do site da CA. Este procedimento de pausa foi informado, clique no botão "OK" para prosseguir.

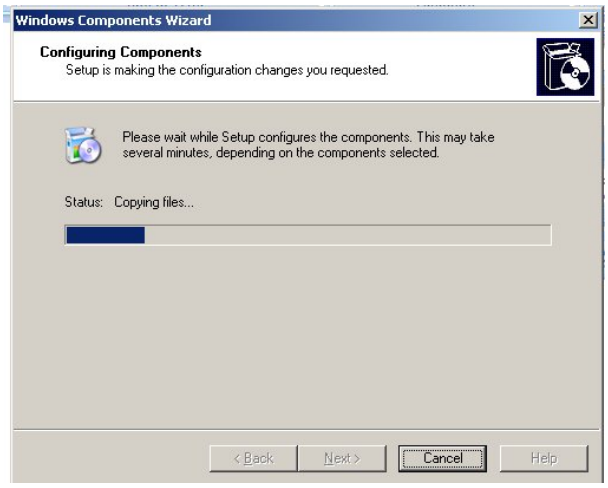
serviço de http

Depois de todas as informações necessárias para a instalação inseriu-se o CD do Microsoft Windows server 2003 para que os arquivos necessários sejam copiados para o seu servidor. insira o CD de instalação e clique no botão "OK".



:Insira o CD de Instalação

Processo de instalação conforme figura em baixo.



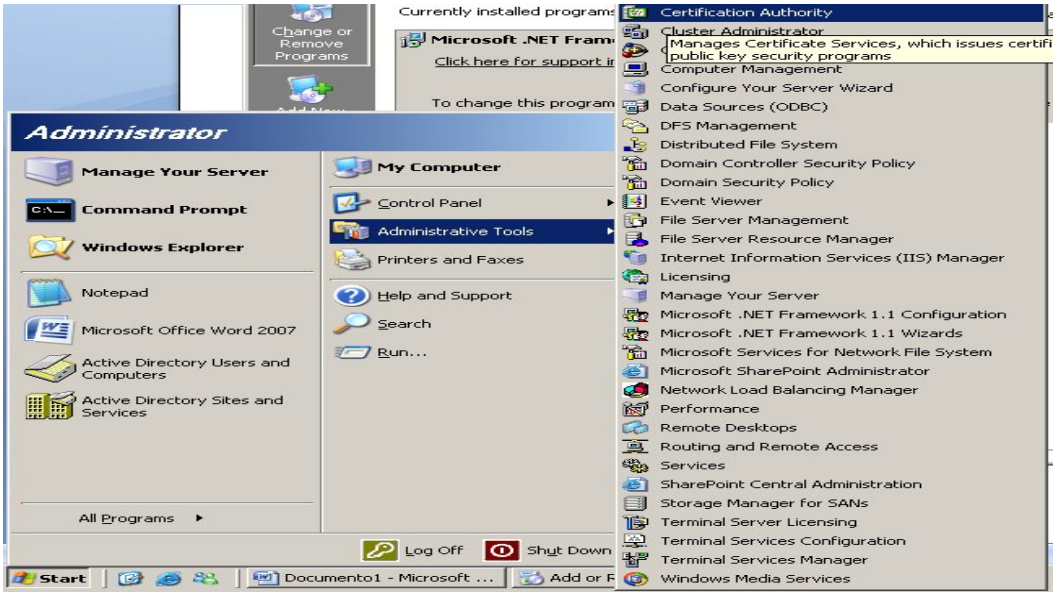
Instalação

Depois da instalação da CA clique no botão "Finish" para fechar a tela de instalação, conforme figura em Baixo.

Instalação concluída

Administrative Tools

Depois da instalação foi certificado se a instalação foi bem sucedida, para isso a basta acessar "Start" > "Administrative Tools" > "Certification Authority", conforme figura em baixo.



A.2 Configuração das permissões

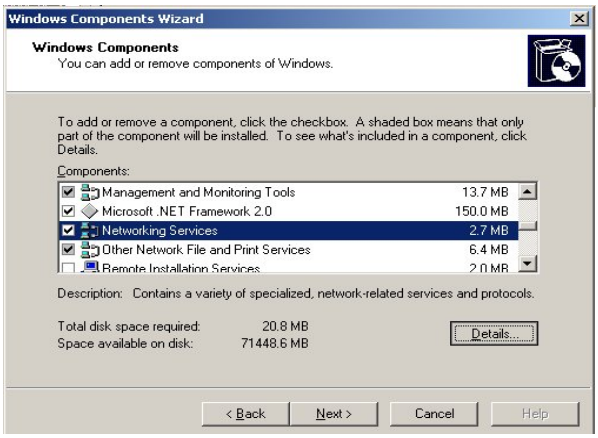
- Abrir Active directory sites and services
- No menu view, seleccione show services Note
- Faça duplo click em publick key services depois em certificate templetes.
- Um de cada vez, faça click com o botão diereito em ClientAuth,user ,domaim controller, and domain Controller Autentication.
- Faça Click em properties, seleccione Security tab,e defina as permissões de registo para os utilizadores autenticados.
- Feche Active Directory Sites services.

A.3 Criação de um domain policy para instalar o certificado nos Clientes

- Abrir o active directory use rand computers, fazer click com o botão no nome de dominio onde o CA pertence, e fazer em propriedades.
- Na aba group palicy, fazer click no policy adequado (por defeito é o default domain policy),e fazer click em edit
- Na janela que aparece selecciona computers configuration,Windows setting,security settings,public,key poilices automatic certificate request settings
- Botão direito em Automatic Certificate request settings,aponta para new e faça click em automatic certificate request
- O wizard do Automatic Certificate request aparece .
- Em certificate templetes, faça click em computer,e avança. O CA criado anteriormente vai aparecer na lista.repete para o domain controlller.
- Sleccione o CA e avança
- Escreva o comando "gpupdate "no command prompt para obter imidiatamente o certificado

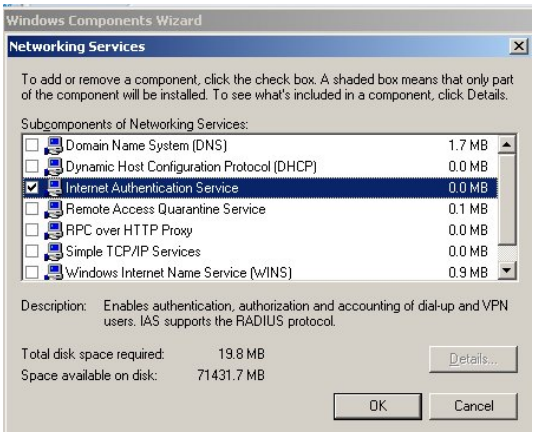
A.4 Instalação de IAS (Internet Authentication Services)

Para adicionar um IAS em um servidor Microsoft Windows 2003 Server utilize o "Windows Components Wizard". Para localizar acesso o "Control Panel" > "Add or Remove Programs" e então escolha "Windows Components" em seguida selecione "Networking Services" e clique em "Details" conforme a fugura em baixo.



Windows Components Wizard

Depois seleccione "Internet Authentication Services" e clique no botão "OK", conforme figura 38.



Internet Autentication Service

Aguarde enquanto o processo de instalação não é concluído, conforme figura em baixo.

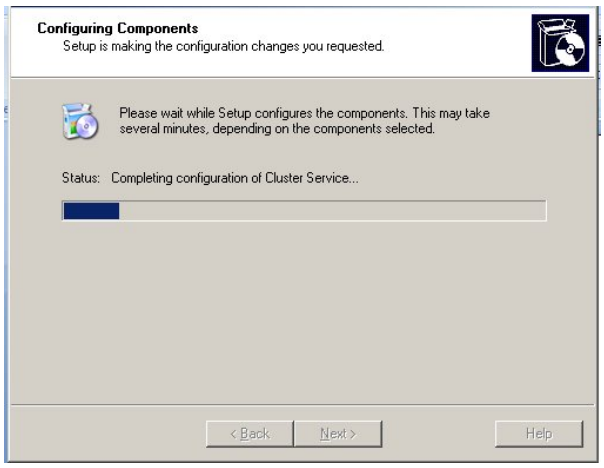


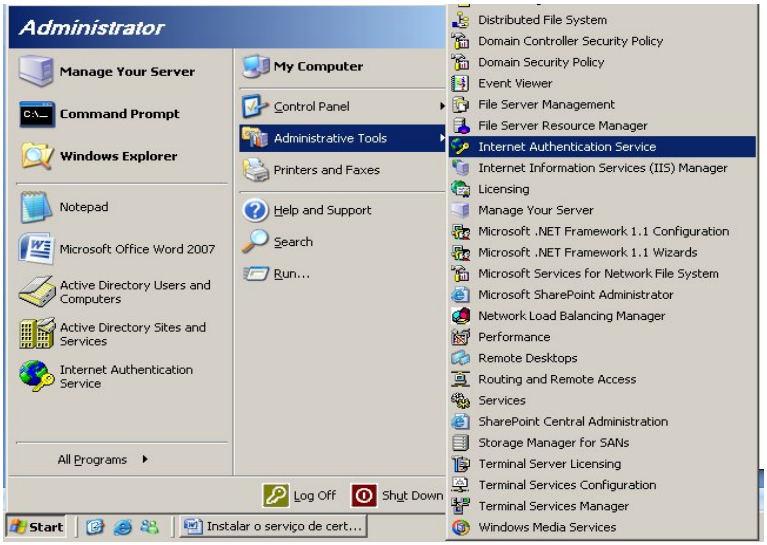
Figura 11:Processo de Instalação

Depois da conclusão clique no botão “Finish” para finalizar a instalação conforme a figura em baixo.

Conclusão

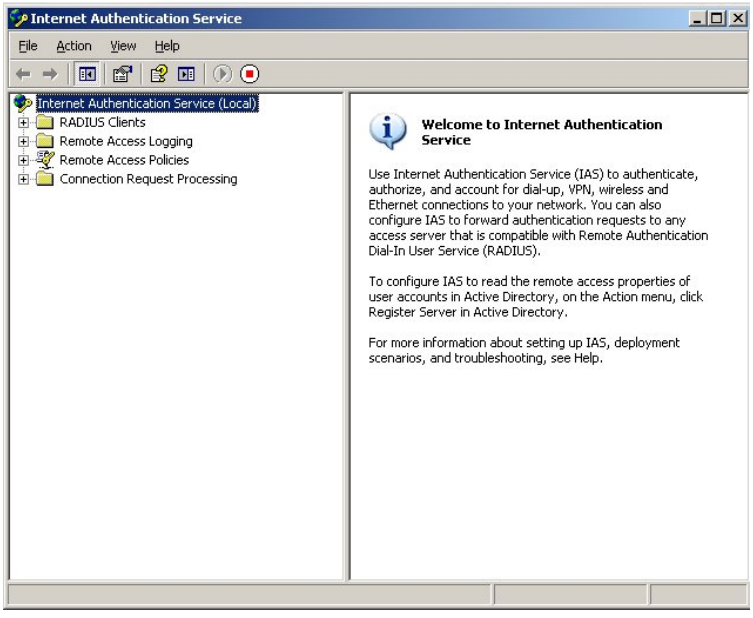
A.5 Configuração do RADIUS

Agora iremos começar o processo de configuração do servidor RADIUS com os Access point da rede. Os Access points serão considerados como clientes do servidor RADIUS e irão encaminhar as solicitações de logon para o servidor. Clique em "Start" > "Administrative Tools" > "Internet Authentication Service" conforme figura em baixo.



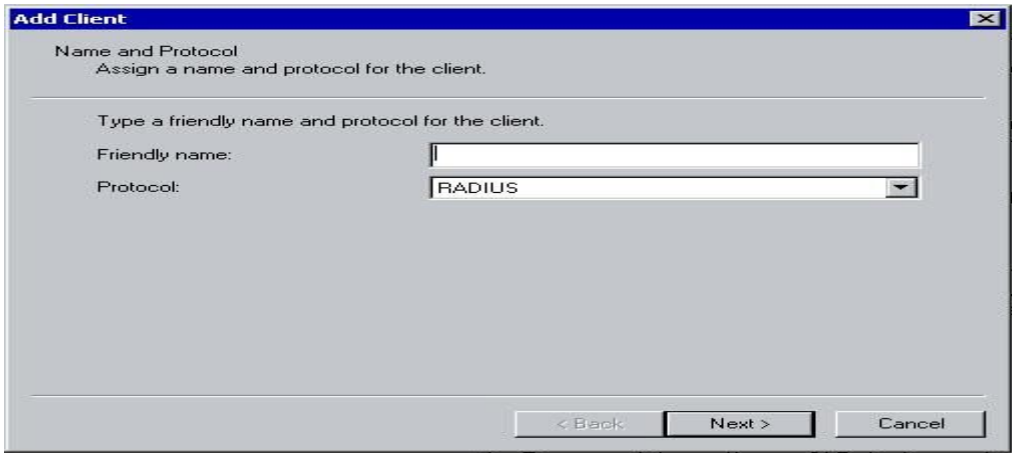
Ferramentas Administrativas

Depois abra a janela de RADIUS conforme figura em baixo.



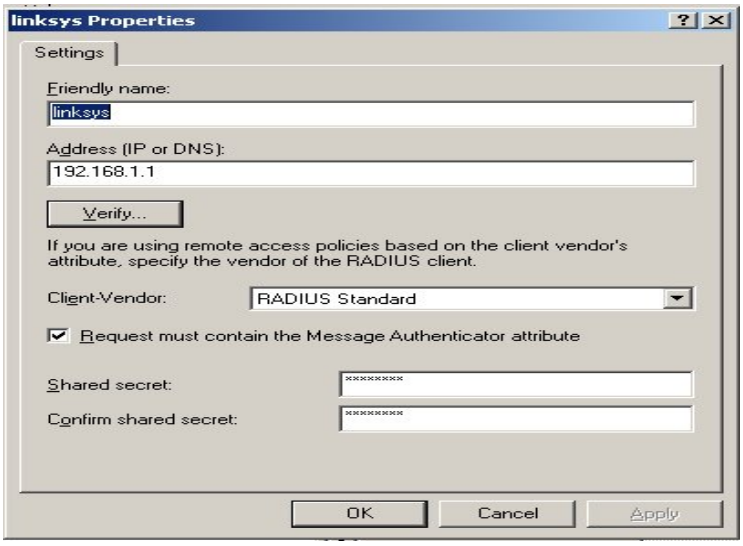
Internet Autentication Service

Clique com o botão direito do Mouse em Internet Authentication Service e seleccione Registrar serviço no Active Directory. Este procedimento irá integrar o serviço de autenticação do RADIUS com o AD. Depois clique com o botão direito em "Clients" e seleccione "New Client". Escreva um nome amigável para registro do access points, Após clique no botão "Next" conforme figura em baixo.



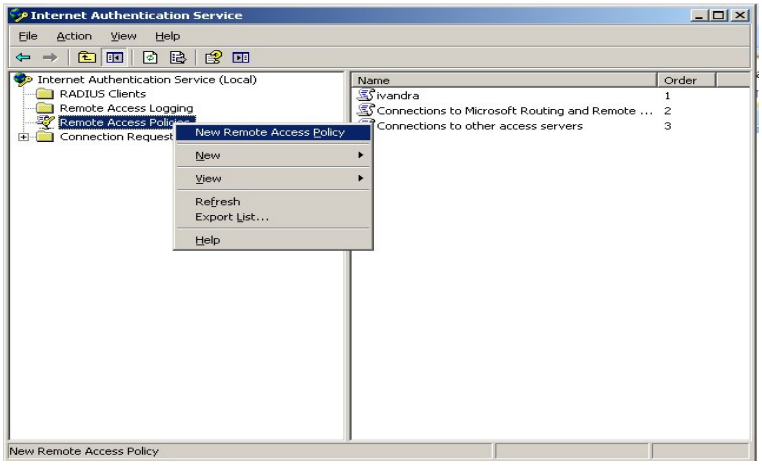
Incluindo o Novo Cliente

Insira o endereço IP do Access Point no campo "Client address (IP or DNS)". Marque a opção "request must Contain the message Autenticator attribute". Inclua uma senha que será o segredo compartilhado entre o RADIUS e o Access Point e depois clique no botão "Finish", para prosseguir conforme figura em baixo.



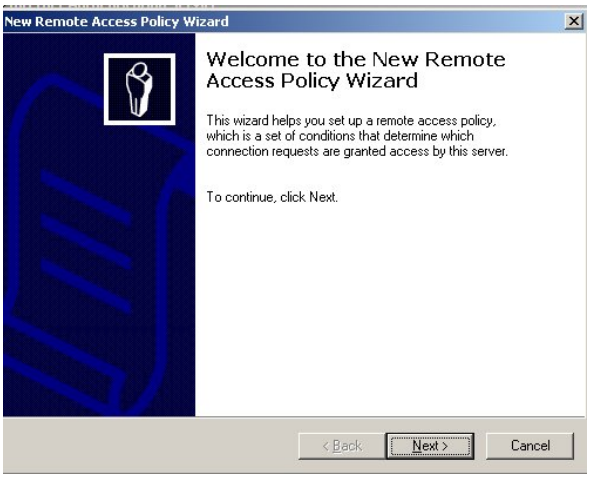
Adicionando o Cliente RADIUS

Para configurar as “Remote Access Polices”, clique no ícone das “Pociles” conforme a figura em baixo.



Seleccionado o acesso remato

Depois da conclusão clique no botão “Finish” para finalizar conforme a figura em baixo.

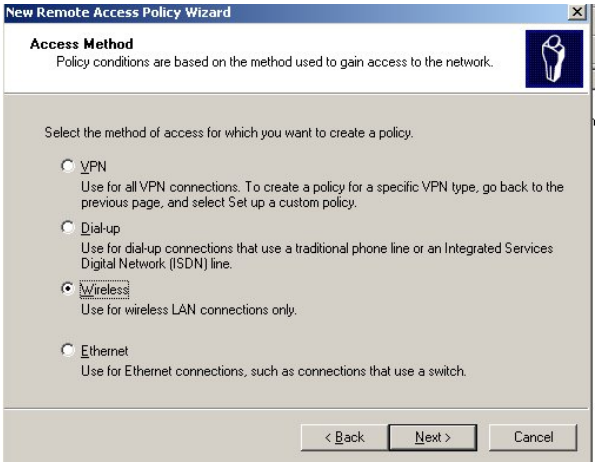


Conclusão

Depois marque a opção “use the wizard to set up a typical policy for a commom scenario”. E escreva o nome de políticas Conforme figura em baixo.

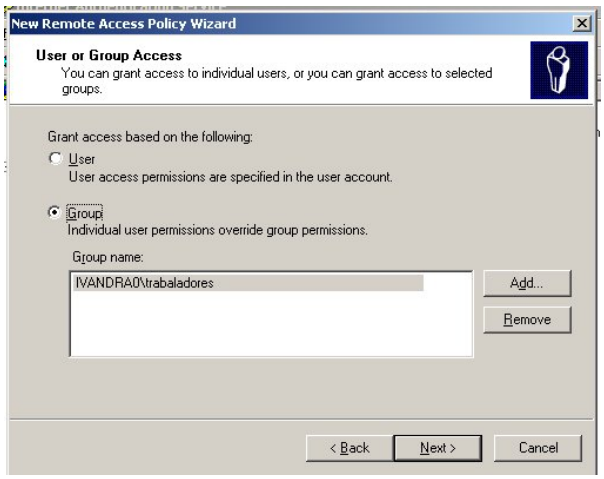
Método de configuração de Politica

Depois marque a opção “Wireless”. Conforme figura em baixo.



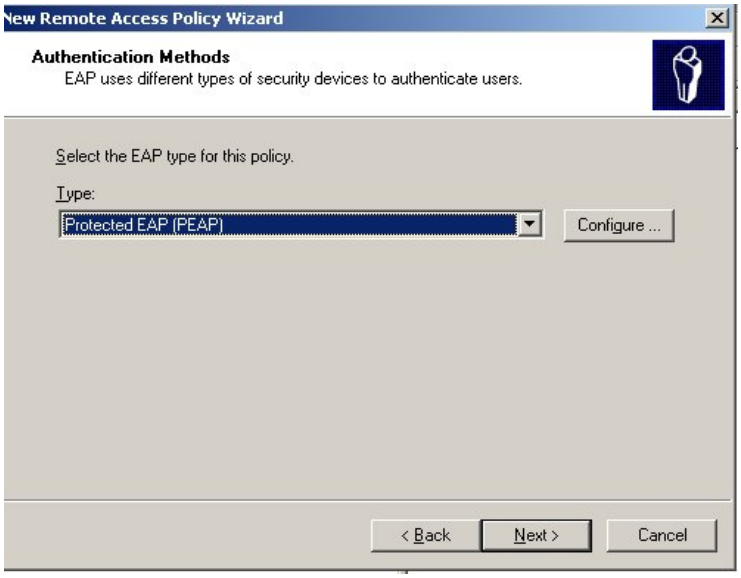
Método de acesso

Seleccione utilizadores ou Grupo no domínio que podem ter acesso a rede depois clique no botão “Next” conforme figura em baixo.



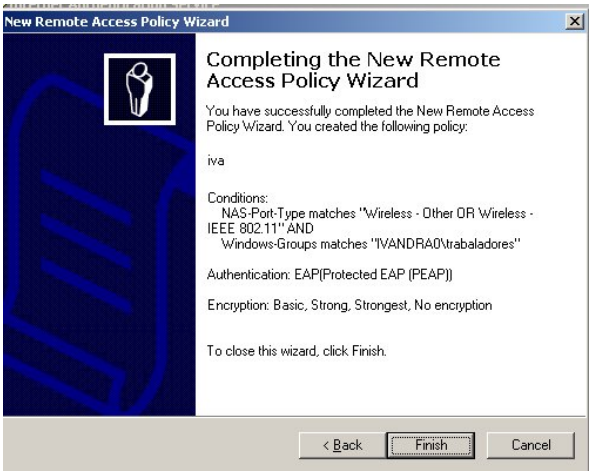
:Grupo de Utilizador

No type escolher a opção”protected EAP (PEAP)” conforme a figura em baixo



:Método de Autenticação

Depois da conclusão clique no botão “Finish” para finalizar conforme a figura em baixo.

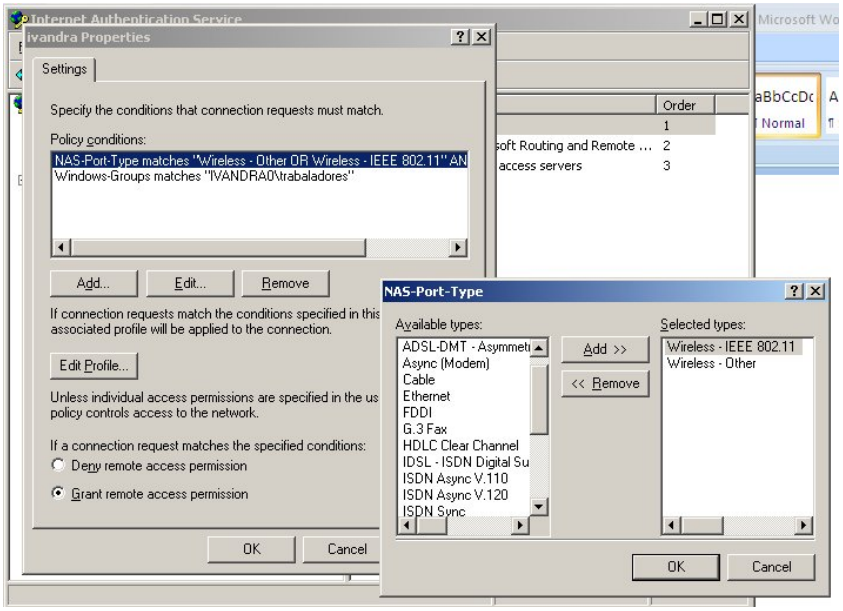


Conclusão

Depois seleccione a Police padrão chamada “Allow access if dial-in permission is enabled” criada pelo servidor, clique com o botão direito para seleccionar propriedades e clique no botão “Edit Profile”.

Na aba “Dial-in Constraints” marque as opções “Restrict Dial-in media:”,

“Wireless – IEEE 802.11” e “Wireless – Other” conforme figura em baixo.



Nas-port-type

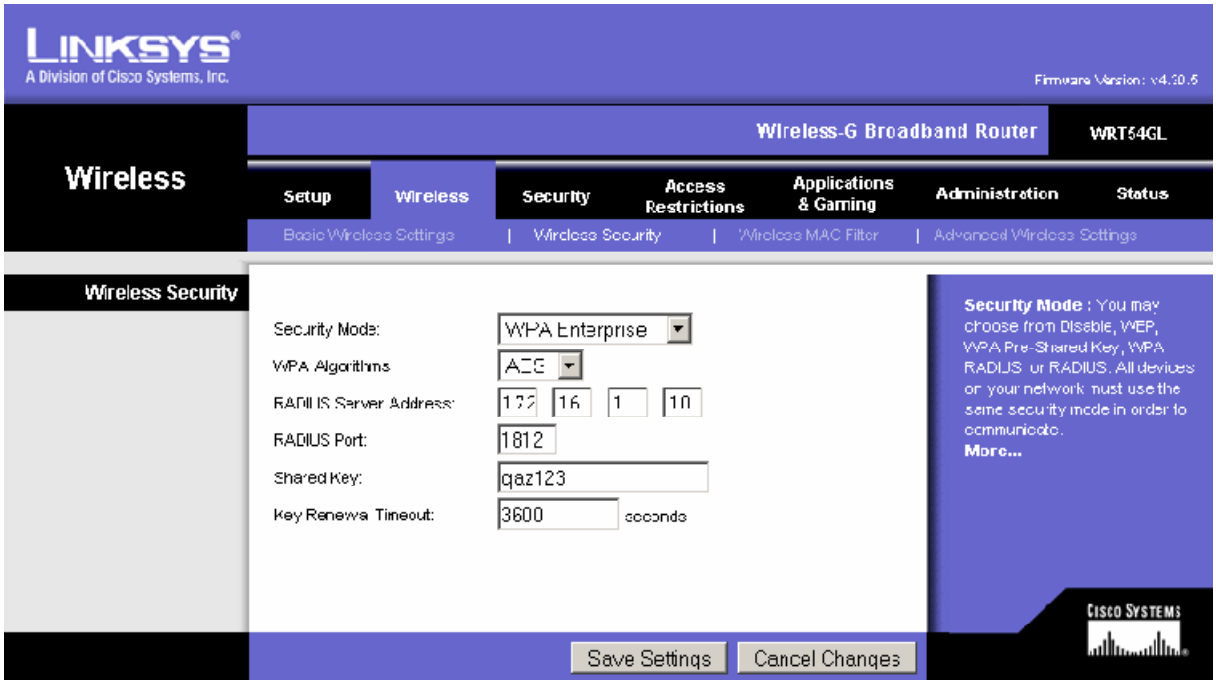
A.6 Configuração do Acess Point

Com o servidor Radius configurado é necessário que o access point repasse a solicitação de autenticação ao servidor. Portanto, para configurar este apontamento no access point é necessário o acesso ao mesmo, normalmente a interface de configuração é via browser, digitando o endereço ip do access point.

Será necessário conter as credencias para o login, procure as opções Wireless e active o padrão 802.11x. As configurações devem ser preenchidas com as opções abaixo.

- Na aba de segurança escolha a opção WAP Enterprise
- Define a encriptação com o método AES
- Insira o IP do Windows 2003 server (O Servidor RADIUS)
- Insira a chave que foi introduzida na IAS
- Server: W2k Radius IP
- Port : 1812
- Radius secret : A mesma palavra que foi digitada no servidor Radius

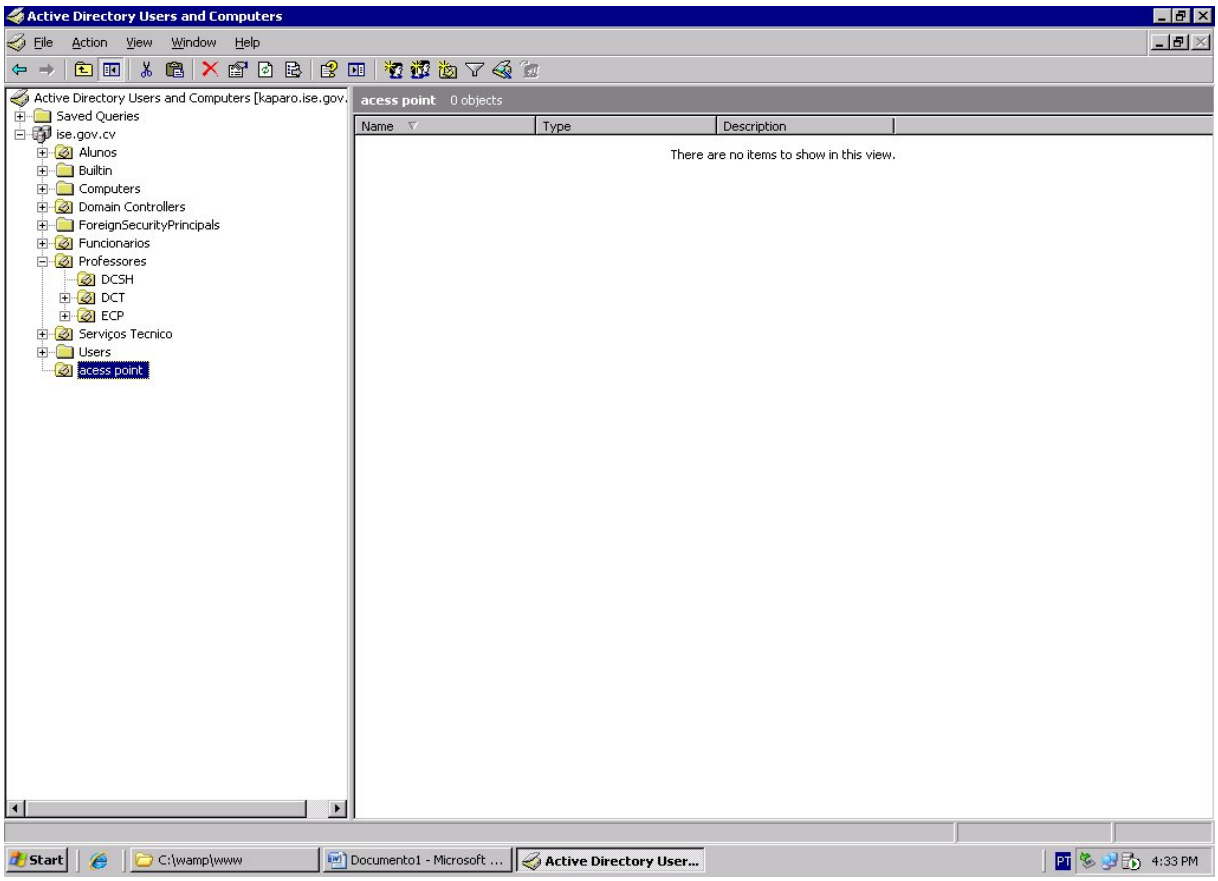
Com forme a figura em baixo



Este documento tem o objectivo de descrever os requisitos necessários para que um aluno ou professor possa utilizar o recurso de wireless da Universidade de Cabo Verde,

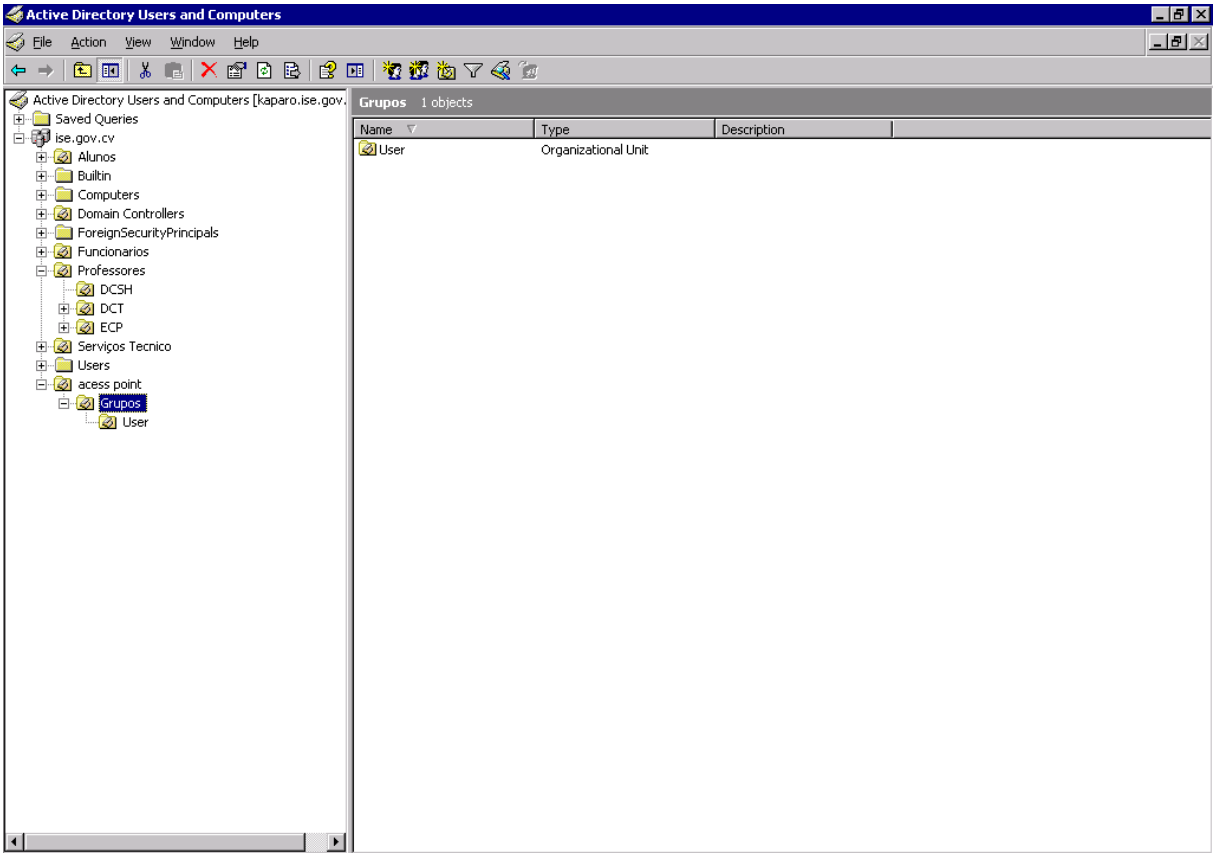
A.7 Criação do utilizador

Será necessário criar o utilizador de domínio para o aluno professor e Funcionário que solicitar acesso ao wireless, pois o certificado é integrado ao utilizador do Active Directory, a criação do utilizador é realizada através da ferramenta de administração do AD chamada "Active Directory Users and Computers" ou simplesmente ADUC. Para acessar o "Active Directory Users and Computers" acesse as ferramentas administrativas, o "Active Directory Users and Computers"



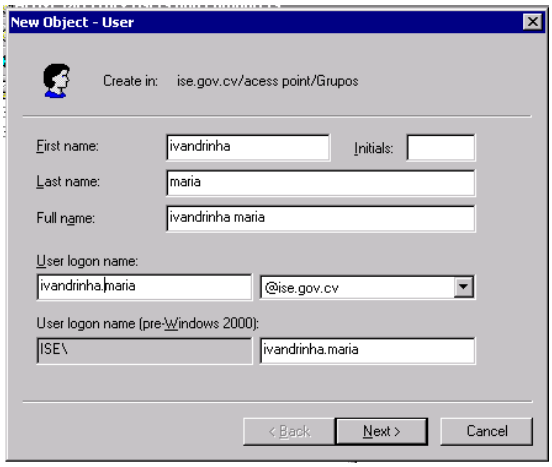
Active Directory Users and Computers

Depois abrir o ADUC abra a OU AccessPoint > Grupos conforme figura em baixo.



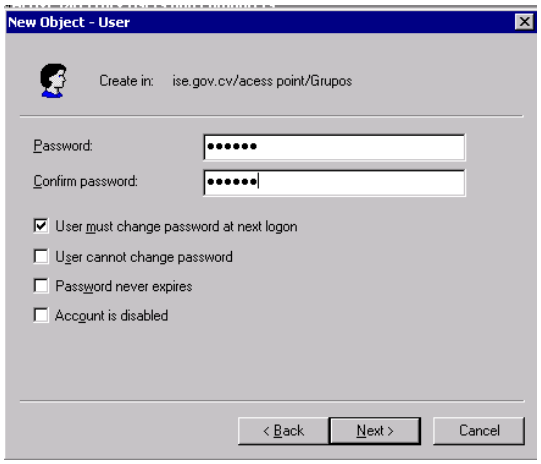
Figuras 12 Acesso o OU Grupos

Clique com botão direito do mouse sobre a OU Users > New > User, será exibida o formulário para criação do utilizador conforme figura em baixo. Preencha com os dados do utilizador que está solicitando o acesso, e clique no botão "Next".



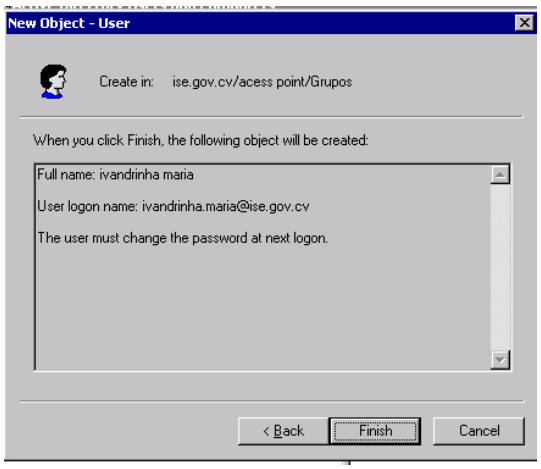
Inserção de Utilizador

Será necessário Criar uma senha para o utilizador, observe na figura 23 que será necessário que o utilizador altere a senha no próximo logon, a senha está sendo cadastrada deverá ser entregue ao utilizador para que o mesmo altere no seu primeiro logon.



Inserção de uma senha temporária

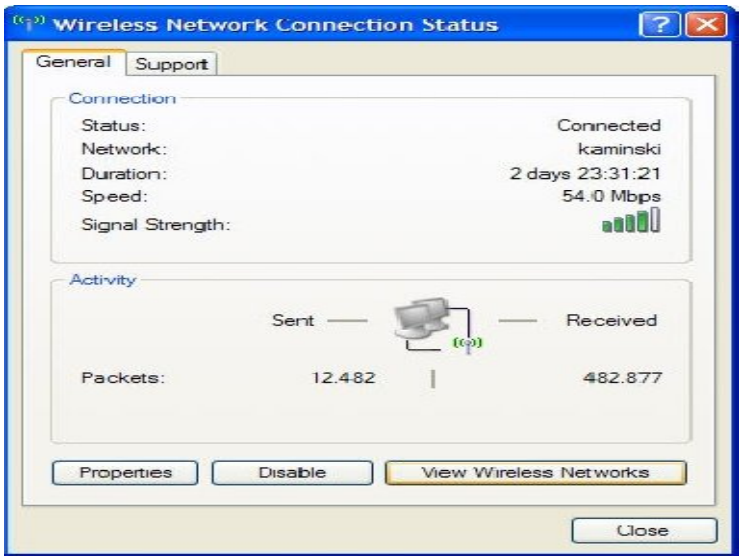
Ao final será informado que o utilizador foi criado e que o mesmo deve alterar a sua senha, clique no botão “Finish” para finalizar conforme figura em baixo.



Conclusão da Criação do Utilizador

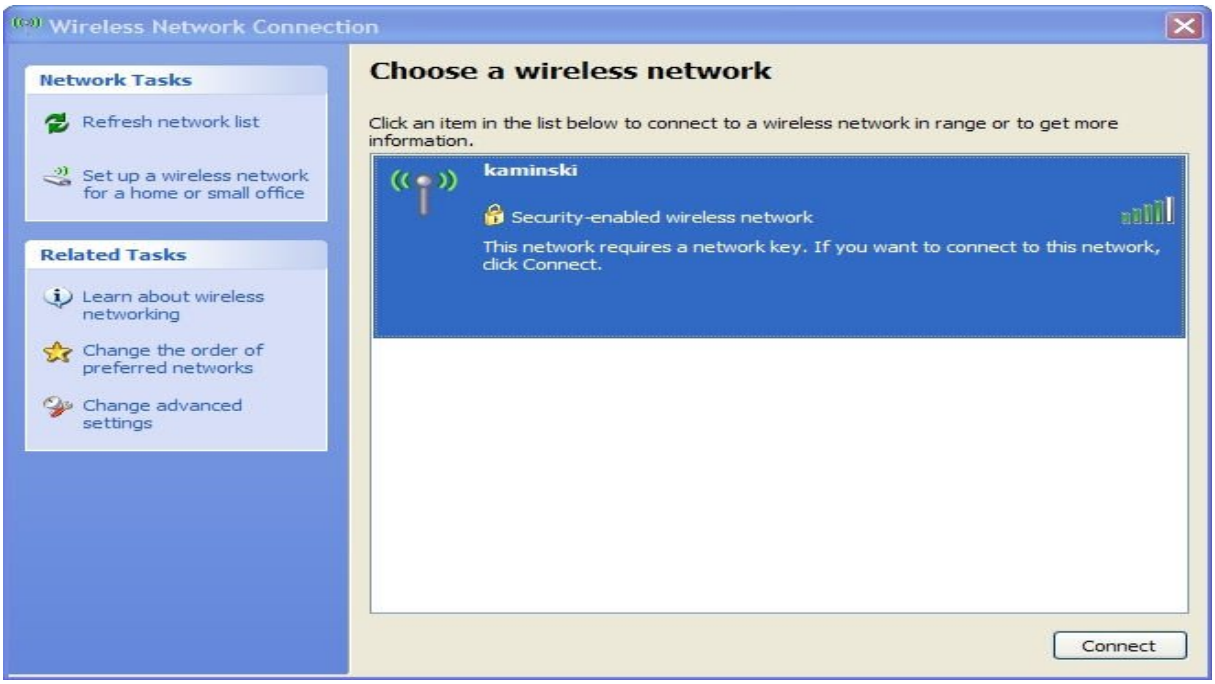
A.8 Configuração do Cliente Windows XP

Para configurar o computador do utilizador basta acessar "Wireless Network Connection" conforme figura em baixo e clicar no botão "View Wireless Networks"
View Wireless Networks"



Wireless Network Connection

Será visualizado a connection wireless disponível, seleccione a rede chamada Linksys e clique em "Conect" conforrme a figura em baixo

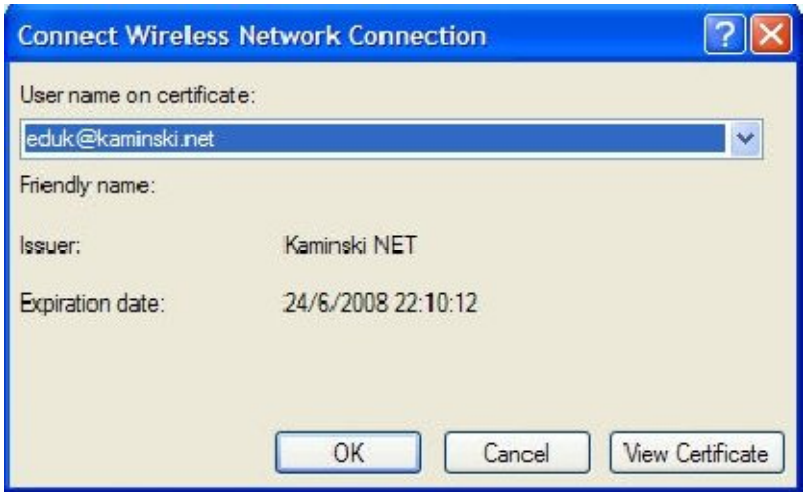


Seleccionando uma rede wireless

Depois seleccionar a rede o computador tentará se comunicar com o Access point, conforme visualiza na figura em baixo

Conectando a Rede

No processo de conexão com a rede será identificado pelo computador que será necessário identificar o certificado para fechar a conexão. Seleccione o certificado, conforme figura em baixo.



Seleccionando o Certificado